



(51) 국제특허분류:

H04W 12/12 (2009.01) H04W 4/00 (2009.01)
H04W 12/02 (2009.01) H04W 4/12 (2009.01)

(21) 국제출원번호:

PCT/KR2016/000375

(22) 국제출원일:

2016년 1월 13일 (13.01.2016)

(25) 출원언어:

한국어

(26) 공개언어:

한국어

(30) 우선권정보:

10-2016-0003957 2016년 1월 12일 (12.01.2016) KR

(71) 출원인: 계명대학교 산학협력단 (INDUSTRY ACADEMIC COOPERATION FOUNDATION KEIMYUNG UNIVERSITY) [KR/KR]; 42601 대구시 달서구 달구벌대로 1095 (신당동), Daegu (KR).

(72) 발명자: 박우길 (PAK, WooGuil); 42601 대구시 달서구 달구벌대로 1095 (신당동), Daegu (KR). 여선기 (YEO, SunKi); 42601 대구시 달서구 달구벌대로 1095 (신당동), Daegu (KR). 차영록 (CHA, YoungRok); 42601 대구시 달서구 달구벌대로 1095 (신당동), Daegu (KR).

(74) 대리인: 김건우 (KIM, Keon Woo); 08507 서울시 금천구 가산디지털1로 168 A-317 (가산동, 우림라이온스밸리), Seoul (KR).

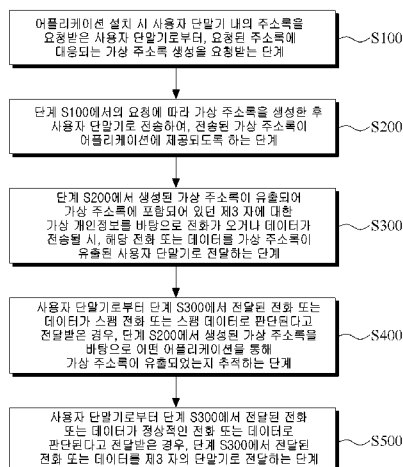
(81) 지정국 (별도의 표시가 없는 한, 가능한 모든 종류의 국내 권리의 보호를 위하여): AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BN, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IR, IS, JP, KE, KG, KN, KP, KZ, LA, LC, LK, LR, LS, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PA, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, SA, SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW.

(84) 지정국 (별도의 표시가 없는 한, 가능한 모든 종류의 국내 권리의 보호를 위하여): ARIPO (BW, GH, GM, KE, LR, LS, MW, MZ, NA, RW, SD, SL, ST, SZ, TZ, UG, ZM, ZW), 유라시아 (AM, AZ, BY, KG, KZ, RU, TJ, TM), 유럽 (AL, AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT, RO, RS, SE, SI, SK, SM, TR),

[다음 쪽 계속]

(54) Title: METHOD FOR DETECTING AND TRACKING ADDRESS BOOK LEAKED THROUGH APPLICATION

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



- S100 ... Step for receiving request for generation of virtual address book corresponding to requested address book, from user terminal requested to provide address book therein when application is installed
- S200 ... Step for generating virtual address book according to request in step S100 and then transmitting virtual address book to user terminal, so as to provide transmitted virtual address book to application
- S300 ... Step for, when virtual address book generated in step S200 is leaked so that call or data is transmitted on basis of virtual personal information of third person included in virtual address book, transferring corresponding call or data to user terminal having virtual address book that is leaked
- S400 ... Step for, when it is informed that call or data transferred from user terminal in step S300 is determined to be spam call or spam data, tracking which application has leaked virtual address book on basis of virtual address book generated in step S200
- S500 ... Step for, when it is informed that call or data transferred from user terminal in step S300 is determined to be normal call or normal data, transferring call or data transferred in step S300 to terminal of third person

(57) Abstract: According to a method for detecting and tracking an address book leaked through an application, which is proposed by the present invention, when a user needs to provide an address book that is in a user cell phone in order to install a specific application on the cell phone, a virtual address book corresponding to the address book in the user cell phone is generated and provided to the corresponding application, so that there is no risk of leakage of the user's actual address book. Thereby, even if the virtual address book is leaked, it is possible to track which application is an application through which the virtual address book is leaked, on the basis of generated virtual address book information.

(57) 요약서: 본 발명에 의해 제안하고 있는 어플리케이션을 통해 유출된 주소록 탐지 및 추적 방법에 따르면, 사용자가 휴대폰에 특정 어플리케이션을 설치하기 위해 사용자 휴대폰 내의 주소록을 제공해야 하는 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.



OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, KM, ML, MR, NE, SN, TD, TG).

공개:
— 국제조사보고서와 함께 (조약 제 21 조(3))

규칙 4.17 에 의한 선언서:

- 신규성을 해치지 아니하는 개시 또는 신규성 상실의 예외에 관한 선언 (규칙 4.17(v))

명세서

발명의 명칭: 어플리케이션을 통해 유출된 주소록 탐지 및 추적 방법

기술분야

- [1] 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.

배경기술

- [2] 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.
- [3]
- [4] 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 방식으로서는, 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.
- [5]
- [6] 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 상세한 설명

기술적 과제

- [7] 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.

과제 해결 수단

- [8] 상기한 목적을 달성하기 위한 본 발명의 특징에 따른, 어플리케이션을 통해 유출된 주소록 탐지 및 추적 방법으로서, 보안서버에서,
- [9] (1) 어플리케이션 설치 시 사용자 단말기 내의 주소록을 요청받은 사용자 단말기로부터, 상기 요청된 주소록에 대응되는 가상 주소록 생성을 요청받는 단계(S100);
- [10] (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);
- [11] (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);
- [12] (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
- [13] (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.
- [14]
- [15] 바람직하게는, 상기 단계 (2)에서,
- [16] 상기 요청된 주소록에 대응되는 가상 주소록을 생성할 때, 상기 어플리케이션 명을 이용하여 가상 주소록을 생성할 수 있다.
- [17]
- [18] 바람직하게는, 상기 단계 (2)에서,
- [19] 상기 어플리케이션마다 각각 다른 가상 주소록을 생성할 수 있다.
- [20]

- [21] 바람직하게는,
[22] 신뢰할 수 있는 어플리케이션 목록을 저장할 수 있다.
[23]
[24] 더욱 바람직하게는, 상기 단계 (2)에서,
[25] 상기 어플리케이션이 상기 저장되어 있는 신뢰할 수 있는 어플리케이션인 경우, 실제 주소록이 제공될 수 있다.
[26]
[27] 바람직하게는, 상기 단계 (3)에서,
[28] 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.
[29]
[30] 바람직하게는,
[31] 스팸 어플리케이션 목록을 저장할 수 있다.
[32]
[33] 더욱 바람직하게는,
[34] 상기 단계 (1)에서 설치하려는 어플리케이션이 상기 저장되어 있는 스팸 어플리케이션인 경우, 상기 사용자 단말기로 경고 메시지를 전송할 수 있다.
[35]
[36] 더욱 바람직하게는, 상기 단계 (4) 이후에,
[37] 상기 가상 주소록을 유출시킨 어플리케이션이 상기 저장되어 있는 스팸 어플리케이션 목록에 업데이트될 수 있다.
[38]
[39] 바람직하게는,
[40] 상기 가상 주소록의 사용가능 기한은 미리 정할 수 있다.
[41]
[42] 상기한 목적을 달성하기 위한 본 발명의 또 다른 특징에 따른, 다른 과정을 통하여 어플리케이션을 통해 유출된 주소록 탐지 및 추적 방법으로서, 보안서버에서,
[43] (1) 어플리케이션 설치 시 사용자 단말기 내의 주소록을 요청받은 사용자 단말기로부터, 상기 요청된 주소록에 대응되는 가상 주소록 생성을 요청받는 단계(S100);
[44] (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);
[45] (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);

[46] (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

[47] (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.

[48]

[49] 바람직하게는, 상기 단계 (2)에서,

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

[51]

[52] 바람직하게는, 상기 단계 (2)에서,

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

[54]

[55] 바람직하게는,

[56] 신뢰할 수 있는 어플리케이션 목록을 저장할 수 있다.

[57]

[58] 더욱 바람직하게는, 상기 단계 (2)에서,

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

[60]

[61] 바람직하게는, 상기 단계 (3)에서,

[62] 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.

[63]

[64] 바람직하게는,

[65] 스팸 어플리케이션 목록을 저장할 수 있다.

[66]

[67] 더욱 바람직하게는,

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

[69]

[70] 더욱 바람직하게는, 상기 단계 (4) 이후에,

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

[72]

[73] 바람직하게는,

[74] 상기 가상 주소록의 사용가능 기한은 미리 정할 수 있다.

발명의 효과

[75] 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

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

[77] 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.

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

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

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

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

[82] 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.

[83] 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.

- [84] 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.
- [85] 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.
- [86] <부호의 설명>
- [87] 100: 사용자 단말기 200: 보안서버
- [88] 300: 제3 자의 단말기
- [89] S100: 어플리케이션 설치 시 사용자 단말기 내의 주소록을 요청받은 사용자 단말기로부터, 요청된 주소록에 대응되는 가상 주소록 생성을 요청받는 단계
- [90] S200: 단계 S100에서의 요청에 따라 가상 주소록을 생성한 후 사용자 단말기로 전송하여, 전송된 가상 주소록이 어플리케이션에 제공되도록 하는 단계
- [91] 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
- [92] 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
- [93] 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
- [94] S100: 어플리케이션 설치 시 사용자 단말기 내의 주소록을 요청받은 사용자 단말기로부터, 요청된 주소록에 대응되는 가상 주소록 생성을 요청받는 단계
- [95] S200: 단계 S100에서의 요청에 따라 가상 주소록을 생성한 후 사용자 단말기로 전송하여, 전송된 가상 주소록이 어플리케이션에 제공되도록 하는 단계
- [96] 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
- [97] 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
- [98] S500: 단계 S400를 통해 추적한 가상 주소록을 유출시킨 어플리케이션을 사용자 단말기에 알리는 단계

발명의 실시를 위한 최선의 형태

[99] 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.

[100]

[101] 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.

[102]

[103] 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.

[104]

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

[106]

[107] 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.

[108]

[109] 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.

[110]

[111] 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.

[112]

[113] 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.

[114]

[115] 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.

[116]

[117] 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.

[118]

[119] 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.

[120]

[121] 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.

[122]

[123] 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.

[124]

[125] 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.

[126]

[127] 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.

[128]

[129] 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.

[130]

[131] 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.

[132]

[133] 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.

[134]

[135] 이하에서는, 상술한 어플리케이션을 통해 유출된 주소록 탐지 및 추적 방법과 다른 과정을 통하여 어플리케이션을 통해 유출된 주소록 탐지 및 추적 방법에 대해 도 10을 참조하여 상세히 설명하기로 한다.

[136]

[137] 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.

[138]

[139] 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.

[140]

[141] 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.

[142]

[143] 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.

[144]

[145] 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.

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 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 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.

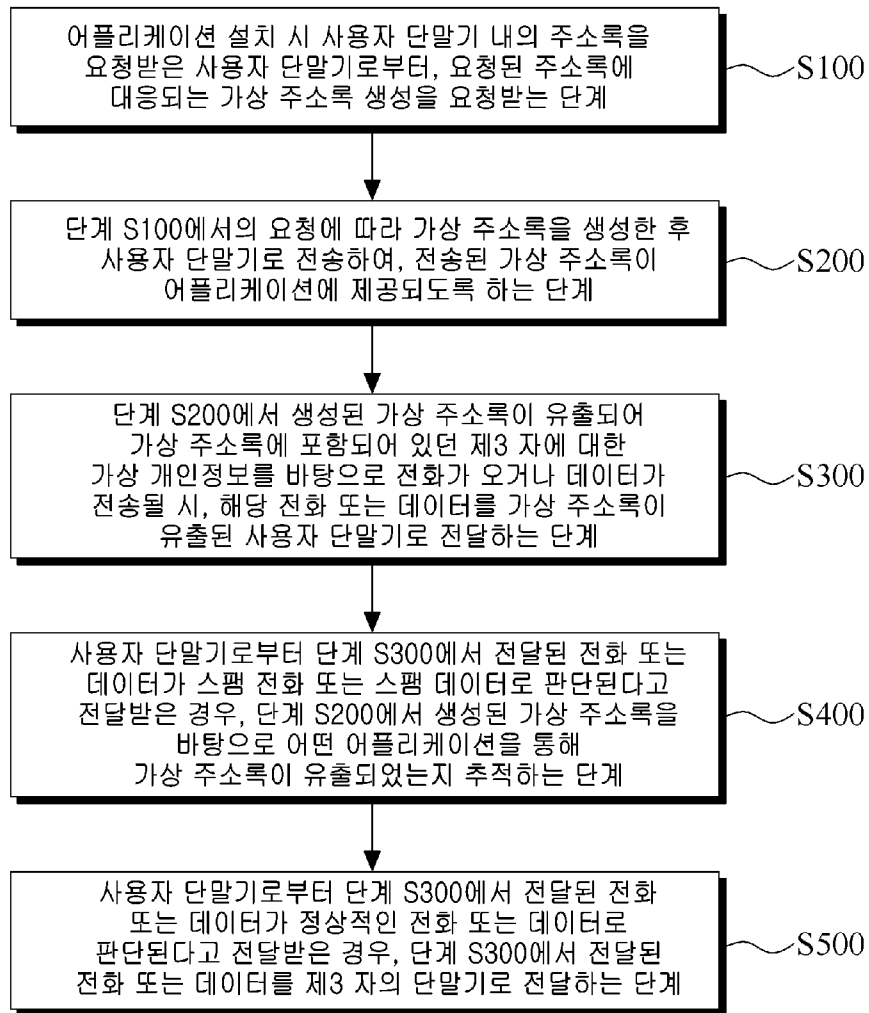
[청구항 16] 제11항에 있어서, 상기 단계 (3)에서, 상기 사용자 단말기(100)로 상기 전화 또는 데이터를 전달할 시, 상기 전화 또는 데이터가 스팸 전화 또는 스팸 데이터일 가능성이 높다는 경고 메시지를 함께 전달할 수 있는 것을 특징으로 하는, 어플리케이션을 통해 유출된 주소록 탐지 및 추적 방법.

[청구항 17] 제11항에 있어서, 스팸 어플리케이션 목록을 저장할 수 있는 것을 특징으로 하는, 어플리케이션을 통해 유출된 주소록 탐지 및 추적 방법.

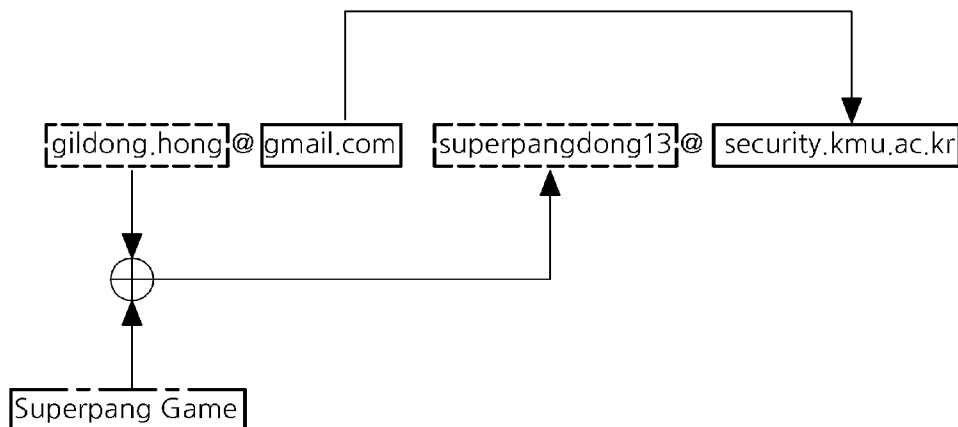
[청구항 18] 제17항에 있어서, 상기 단계 (1)에서 설치하려는 어플리케이션이 상기 저장되어 있는 스팸 어플리케이션인 경우, 상기 사용자 단말기(100)로 경고 메시지를 전송할 수 있는 것을 특징으로 하는, 어플리케이션을

- [청구항 19] 통해 유출된 주소록 탐지 및 추적 방법.
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.

[Fig. 1]



[Fig. 2]



[Fig. 3]



[Fig. 4]



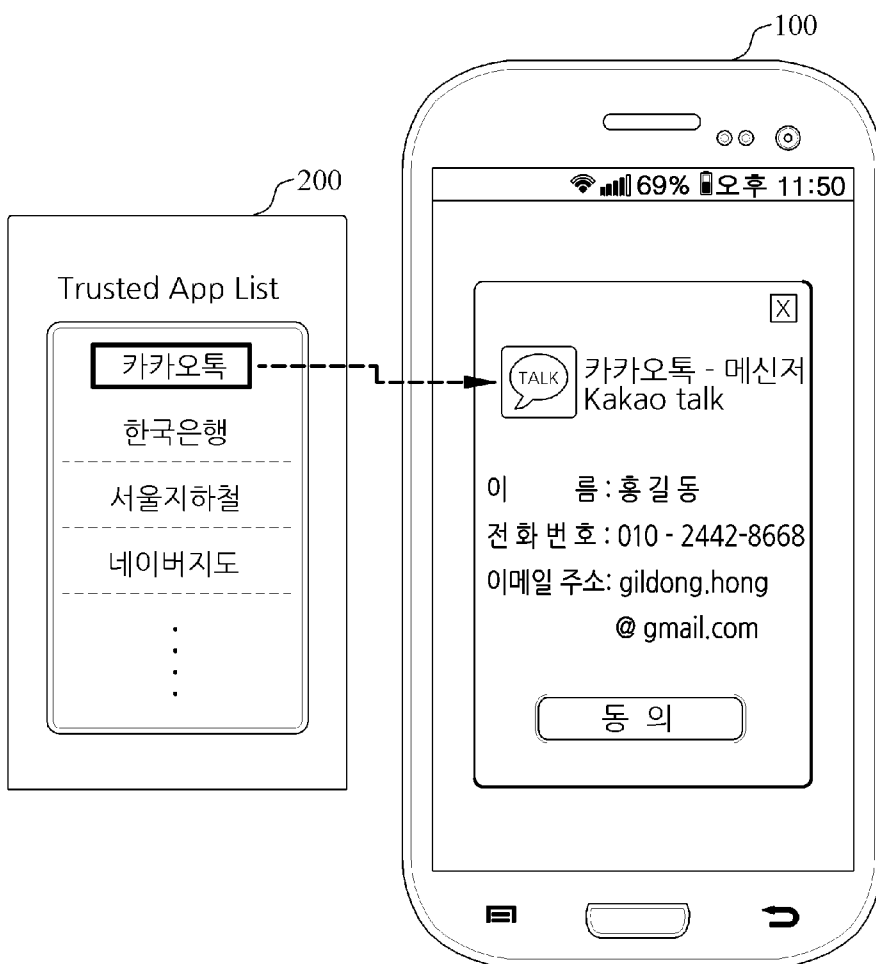
[Fig. 5]



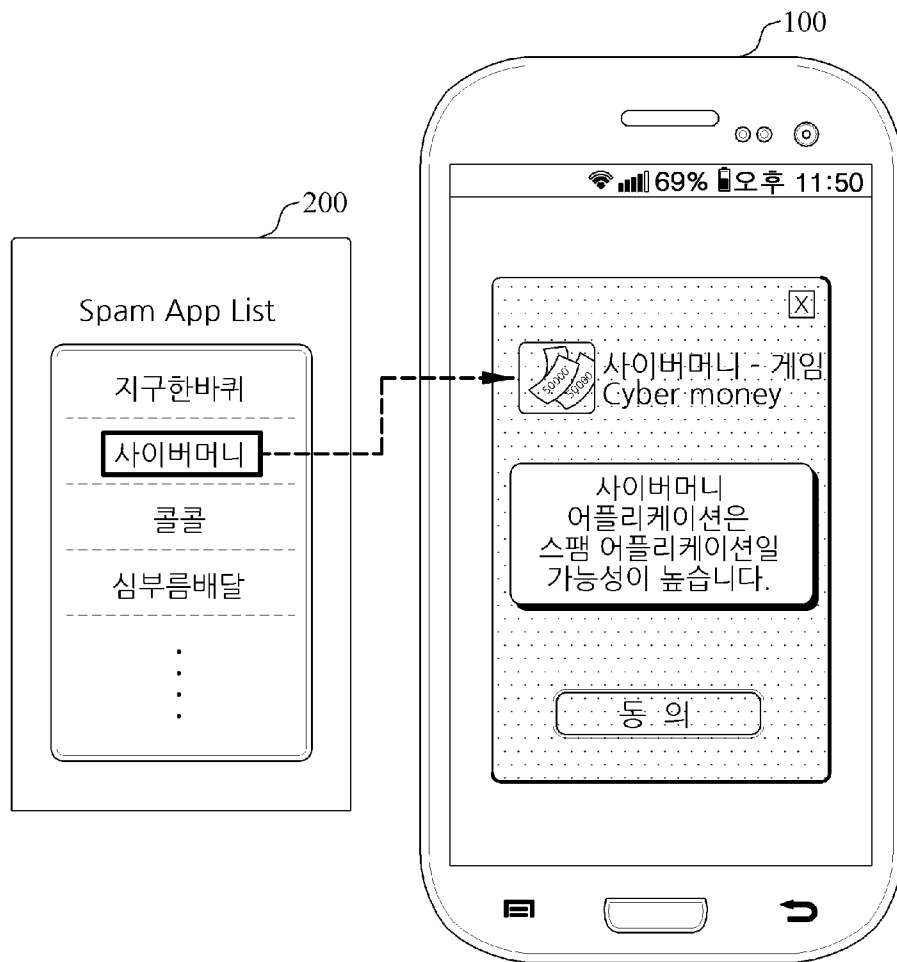
[Fig. 6]



[Fig. 7]



[Fig. 8]



[Fig. 9]

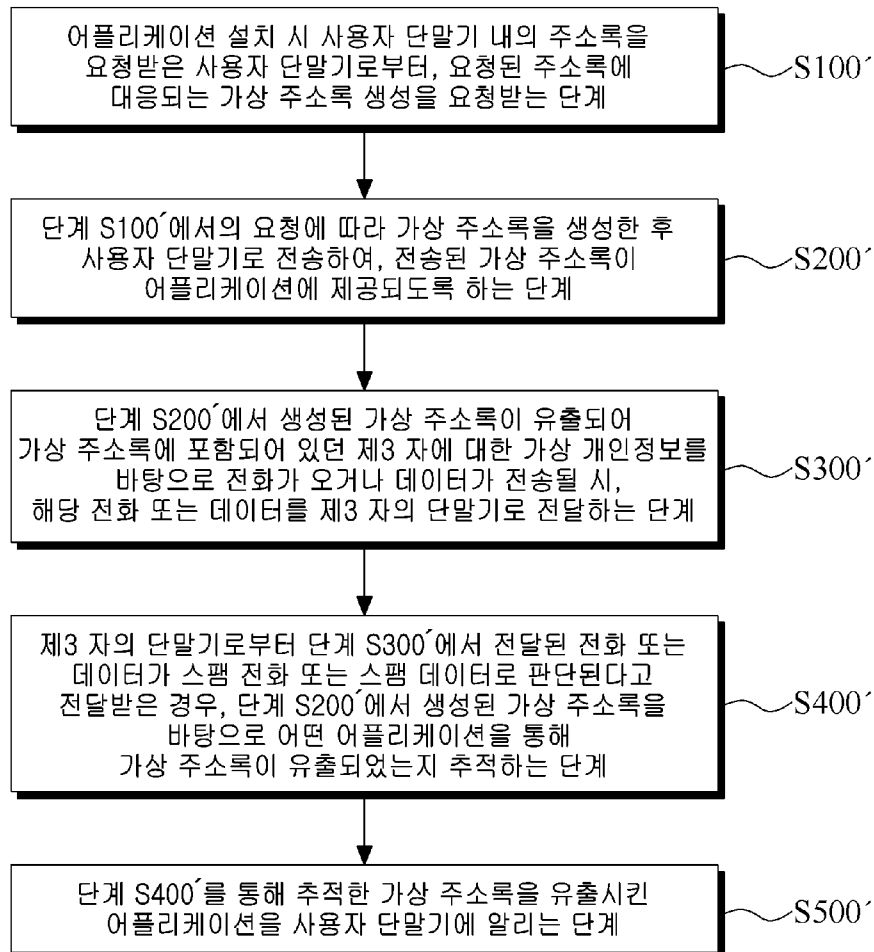


(a)



(b)

[Fig. 10]



INTERNATIONAL SEARCH REPORT

International application No.

PCT/KR2016/000375

A. CLASSIFICATION OF SUBJECT MATTER

H04W 12/12(2009.01)i, H04W 12/02(2009.01)i, H04W 4/00(2009.01)i, H04W 4/12(2009.01)i

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

H04W 12/12; H04W 4/12; G06F 21/56; H04W 4/16; H04W 88/18; H04W 8/18; H04W 12/02; H04W 4/00

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Korean Utility models and applications for Utility models: IPC as above

Japanese Utility models and applications for Utility models: IPC as above

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

eKOMPASS (KIPO internal) & Keywords: application, virtual address book, virtual personal information, security server, user, third party, terminal, tracking, prank call, junk data

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	CHOI, Young Seok et al., "Study to Detect and Block Leakage of Personal Information: Android-platform Environment", Journal of The Korea Institute of Information Security & Cryptology, vol. 23, no. 4, pp. 757-766, August 2013 (http://www.dbpia.co.kr/Journal/ArticleDetail/NODE02238410) See page 764; and figures 7-8.	1-20
A	KR 10-2015-0129538 A (SK PLANET CO., LTD.) 20 November 2015 See paragraphs [0080]-[0082]; claim 1; and figure 5.	1-20
A	KR 10-2009-0086377 A (KOO, Kyeong Hoon) 12 August 2009 See paragraphs [0023]-[0028]; and figure 2.	1-20
A	WO 2015-056885 A1 (ESTSOFT CORP. et al.) 23 April 2015 See paragraphs [76]-[83]; and figure 9.	1-20
A	KR 10-2012-0071162 A (KT CORPORATION) 02 July 2012 See paragraphs [0038]-[0045]; and figure 2.	1-20



Further documents are listed in the continuation of Box C.



See patent family annex.

* Special categories of cited documents:

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier application or patent but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art

"&" document member of the same patent family

Date of the actual completion of the international search

11 OCTOBER 2016 (11.10.2016)

Date of mailing of the international search report

11 OCTOBER 2016 (11.10.2016)

Name and mailing address of the ISA/KR



Korean Intellectual Property Office
Government Complex-Daejeon, 189 Sconsa-ro, Daejeon 302-701,
Republic of Korea

Facsimile No. +82-42-481-8578

Authorized officer

Telephone No.

INTERNATIONAL SEARCH REPORT

International application No.

PCT/KR2016/000375

C (Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT		
Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	PAK, Wooguik et al., "Detecting and Tracing Leaked Private Phone Number Data in Android Smartphones", iCOIN 2015, The 29th International Conference on Information Networking, 12-14 January 2015 See section II. ※ The above document is a known document declaring exceptions to lack of novelty by the applicant.	1-20

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No.

PCT/KR2016/000375

Patent document cited in search report	Publication date	Patent family member	Publication date
KR 10-2015-0129538 A	20/11/2015	NONE	
KR 10-2009-0086377 A	12/08/2009	NONE	
WO 2015-056885 A1	23/04/2015	KR 10-2015-0044490 A	27/04/2015
KR 10-2012-0071162 A	02/07/2012	NONE	

A. 발명이 속하는 기술분류(국제특허분류(IPC))

H04W 12/12(2009.01)i, H04W 12/02(2009.01)i, H04W 4/00(2009.01)i, H04W 4/12(2009.01)i

B. 조사된 분야

조사된 최소문헌(국제특허분류를 기재)

H04W 12/12; H04W 4/12; G06F 21/56; H04W 4/16; H04W 88/18; H04W 8/18; H04W 12/02; H04W 4/00

조사된 기술분야에 속하는 최소문헌 이외의 문헌

한국등록실용신안공보 및 한국공개실용신안공보: 조사된 최소문헌란에 기재된 IPC

일본등록실용신안공보 및 일본공개실용신안공보: 조사된 최소문헌란에 기재된 IPC

국제조사에 이용된 전산 데이터베이스(데이터베이스의 명칭 및 검색어(해당하는 경우))

eKOMPASS(특허청 내부 검색시스템) & 키워드: 어플리케이션, 가상 주소록, 가상 개인정보, 보안서버, 사용자, 제3자, 단말기, 추적, 스팸 전화, 스팸 데이터

C. 관련 문헌

카테고리*	인용문헌명 및 관련 구절(해당하는 경우)의 기재	관련 청구항
A	최영석 등, `개인정보 유출 탐지 및 차단에 관한 연구 : 안드로이드 플랫폼 환경`, 정보보호학회논문지, 제23권, 제4호, pp. 757-766, 2013.08 (http://www.dbpia.co.kr/Journal/ArticleDetail/NODE02238410) 페이지 764; 및 도면 7-8 참조.	1-20
A	KR 10-2015-0129538 A (에스케이플래닛 주식회사) 2015.11.20 단락 [0080]-[0082]; 청구항 1; 및 도면 5 참조.	1-20
A	KR 10-2009-0086377 A (구경훈) 2009.08.12 단락 [0023]-[0028]; 및 도면 2 참조.	1-20
A	WO 2015-056885 A1 ((주)이스트소프트 등) 2015.04.23 단락 [76]-[83]; 및 도면 9 참조.	1-20
A	KR 10-2012-0071162 A (주식회사 케이티) 2012.07.02 단락 [0038]-[0045]; 및 도면 2 참조.	1-20

☒ 추가 문헌이 C(계속)에 기재되어 있습니다.

☒ 대응특허에 관한 별지를 참조하십시오.

* 인용된 문헌의 특별 카테고리:

“A” 특별히 관련이 없는 것으로 보이는 일반적인 기술수준을 정의한 문헌

“T” 국제출원일 또는 우선일 후에 공개된 문헌으로, 출원과 상충하지 않으며 발명의 기초가 되는 원리나 이론을 이해하기 위해 인용된 문헌

“E” 국제출원일보다 빠른 출원일 또는 우선일을 가지나 국제출원일 이후에 공개된 선출원 또는 특허 문헌

“X” 특별한 관련이 있는 문헌. 해당 문헌 하나만으로 청구된 발명의 신규성 또는 진보성이 없는 것으로 본다.

“L” 우선권 주장에 의문을 제기하는 문헌 또는 다른 인용문헌의 공개일 또는 다른 특별한 이유(이유를 명시)를 밝히기 위하여 인용된 문헌

“Y” 특별한 관련이 있는 문헌. 해당 문헌이 하나 이상의 다른 문헌과 조합하는 경우로 그 조합이 당업자에게 자명한 경우 청구된 발명은 진보성이 없는 것으로 본다.

“O” 구두 개시, 사용, 전시 또는 기타 수단을 언급하고 있는 문헌

“&” 동일한 대응특허문헌에 속하는 문헌

“P” 우선일 이후에 공개되었으나 국제출원일 이전에 공개된 문헌

국제조사의 실제 완료일

2016년 10월 11일 (11.10.2016)

국제조사보고서 발송일

2016년 10월 11일 (11.10.2016)

ISA/KR의 명칭 및 우편주소

대한민국 특허청
(35208) 대전광역시 서구 청사로 189,
4동 (둔산동, 정부대전청사)

팩스 번호 +82-42-481-8578

심사관

양정록

전화번호 +82-42-481-5709



C(계속). 관련 문헌		
카테고리*	인용문헌명 및 관련 구절(해당하는 경우)의 기재	관련 청구항
X	WOOGUIL PAK 등, `Detecting and tracing leaked private phone number data in Android smartphones`, iCOIN 2015, The 29th International Conference on Information Networking, 2015.01.12-14 섹션 II 참조. ※ 위 문헌은 출원인이 신규성 상실의 예외로서 선언한 공지문헌임.	1-20

국제조사보고서에서 인용된 특허문헌	공개일	대응특허문헌	공개일
KR 10-2015-0129538 A	2015/11/20	없음	
KR 10-2009-0086377 A	2009/08/12	없음	
WO 2015-056885 A1	2015/04/23	KR 10-2015-0044490 A	2015/04/27
KR 10-2012-0071162 A	2012/07/02	없음	