(19) 대한민국특허청(KR)
(12) 공개특허공보(A)

(11) 공개번호 10-2015-0066271
(43) 공개일자 2015년06월16일

(51) 국제특허분류(Int. Cl.)
G06F 21/50 (2013.01) *G06F 17/00* (2006.01)
(21) 출원번호 10-2013-0151625
(22) 출원일자 2013년12월06일
심사청구일자 2013년12월06일

(71) 출원인
충남대학교산학협력단
대전광역시 유성구 대학로 99 (궁동, 충남대학교)
(72) 발명자
류재철
대전광역시 유성구 어은로 57 한빛아파트 132-801
김동욱
대전광역시 유성구 신성로61번안길 24 202호
김상우
대전광역시 유성구 대학로145번길 22 204호
(74) 대리인
권혁수, 송윤호

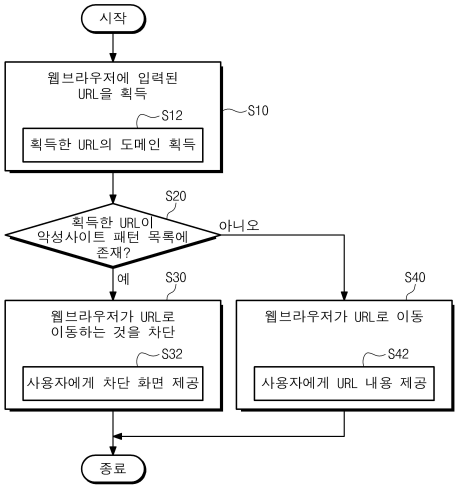
전체 청구항 수 : 총 10 항

(54) 발명의 명칭 **안드로이드 플랫폼에서 악성 사이트 차단 방법 및 이를 이용한 휴대 단말기**

(57) 요 약

본 발명은 웹브라우저에 입력된 URL을 획득하는 단계, URL을 저장된 악성 사이트 패턴 목록과 비교하는 단계 및 웹브라우저가 URL로 이동하는 것을 차단하는 단계를 포함하는 악성 사이트 차단 방법에 관한 것이다.

대 표 도 - 도1



이 발명을 지원한 국가연구개발사업
과제고유번호 H0301-12-4008/ 1415123340
부처명 지식경제부
연구관리전문기관 정보통신산업진흥원
연구사업명 대학 IT연구센터 육성·지원사업
연구과제명 클라우드 환경의 스마트 기기와 서비스 보안 기술 개발 및연구 인력양성
기 여 율 1/1
주관기관 숭실대학교 산학협력단
연구기간 2013.01.01 ~ 2013.12.31

명 세 서

청구범위

청구항 1

웹브라우저에 입력된 URL을 획득하는 단계;

상기 URL을 저장된 악성 사이트 패턴 목록과 비교하는 단계; 및

상기 웹브라우저가 상기 URL로 이동하는 것을 차단하는 단계;

를 포함하는 악성 사이트 차단 방법.

청구항 2

제1항에 있어서,

상기 URL을 획득하는 단계는

상기 URL의 도메인을 획득하는 단계;

를 포함하는 악성 사이트 차단 방법.

청구항 3

제1항에 있어서,

상기 악성 사이트 패턴 목록을 획득하는 단계; 를 더 포함하고,

상기 악성 사이트 패턴 목록을 획득하는 단계는

APWG(Anti Phishing Working Group)으로부터 주기적으로 패턴 파일을 제공받는 단계; 및

사용자들로부터 악성 사이트를 수집하는 단계;

중 적어도 어느 하나를 포함하는 악성 사이트 차단 방법.

청구항 4

제3항에 있어서,

상기 악성 사이트 패턴 목록을 획득하는 단계는

상기 제공받은 패턴 파일 또는 상기 수집한 악성 사이트를 분석하여 URL을 분석하는 단계;

를 더 포함하는 악성 사이트 차단 방법.

청구항 5

제1항에 있어서,

상기 차단하는 단계는

상기 URL이 상기 악성 사이트 패턴 목록에 포함되는 경우 사용자에게 차단 화면을 제공하는 단계; 또는

상기 URL이 상기 악성 사이트 패턴 목록에 포함되지 않는 경우 웹브라우저가 상기 URL로 이동하는 단계;

중 적어도 어느 하나를 포함하는 악성 사이트 차단 방법.

청구항 6

제1항 내지 제5항의 방법 중 어느 한 항의 방법을 컴퓨터에서 실행시키기 위한 프로그램을 기록한 컴퓨터가 읽을 수 있는 기록 매체

청구항 7

표시부 및 제어부를 포함하는 휴대 단말기에 있어서,

상기 제어부는 웹브라우저에 URL이 입력되면 상기 웹브라우저가 URL로 이동하는 것을 차단하고,

상기 URL을 악성 사이트 패턴 목록과 비교하여 상기 URL이 상기 악성 사이트 패턴 목록에 포함되지 않은 경우, 상기 표시부가 상기 웹브라우저가 상기 URL로 이동한 결과를 제공하도록 제어하는 휴대 단말기.

청구항 8

제7항에 있어서,

상기 제어부는 상기 표시부에 다른 어플리케이션이 실행 중일 때는 백그라운드에서 서비스로써 동작하는 휴대 단말기.

청구항 9

제7항에 있어서,

상기 제어부는 APWG로부터 주기적으로 패턴 파일을 제공받거나

사용자들로부터 악성 사이트를 수집하여 상기 악성 사이트 패턴 목록을 획득하는 휴대 단말기.

청구항 10

제9항에 있어서,

상기 제어부는 획득한 상기 악성 사이트 패턴 목록을 분석하여 URL을 획득하고,

상기 입력된 URL이 상기 악성 사이트 패턴 목록에 포함되면 상기 표시부가 차단 화면을 제공하도록 제어하는 휴대 단말기.

발명의 설명

기 술 분 야

[0001] 본 발명은 안드로이드 플랫폼에서 악성 사이트 차단 방법 및 이를 이용한 휴대 단말기에 대한 것이다.

배 경 기 술

[0002] 스마트폰, 태블릿과 같은 스마트 기기의 사용자수는 2013년 1월 말을 기준으로 3300만 명이 넘는다. 스마트 기기의 사용자가 늘어남에 따라 스마트 기기를 대상으로 하는 모바일 오피스, 금융 서비스, 모바일 전자정부 등과 같은 생산성이나 사용자 편의를 위한 서비스들이 대거 등장하였다. 이에 따라, 중요한 정보들이 스마트 기기를 통해 다루어져 스마트 기기를 대상으로 하는 악성 행위가 꾸준히 증가하고 있다. 특히, 스마트 기기를 대상으로

하는 유해 사이트, 악성코드 배포 사이트, 피싱(Phishing) 사이트 등이 증가하고, 이로 인한 피해 사례가 꾸준히 발생하고 있어, 스마트 기기에 대한 보안 문제는 중요한 이슈가 되고 있다. 특히, 국내에서 사용하는 스마트 기기의 90% 이상이 안드로이드 플랫폼을 이용하고 있어, 안드로이드 플랫폼에서의 악성 사이트 차단 방법의 필요성이 제기되고 있다.

[0003] 종래에는 네트워크 방화벽 또는 PC방화벽을 통해 악성 사이트를 차단하였다. 네트워크 방화벽은 네트워크 중간에 패킷을 검사하는 하드웨어 기반 차단 방법이고, PC 방화벽은 PC에서 커널 소프트웨어로 네트워크 패킷을 검사하는 방법이다. 하지만, 주로 무선 통신을 이용하는 스마트 기기의 특성상 무선 통신망에 하드웨어 기반 네트워크 방화벽을 모두 설치하기에는 한계가 있고, 스마트 기기 기반의 소프트웨어 방화벽은 권한 문제로 인해 일반적인 방법으로는 악성 사이트 접근을 차단할 수 없다.

발명의 내용

해결하려는 과제

[0004] 본 발명의 목적은 안드로이드 플랫폼을 이용하는 스마트 기기에서, 웹브라우저를 이용한 악성 사이트 방문을 차단하는 데 있다.

[0005] 본 발명의 기술적 과제는 이상에서 언급한 기술적 과제들로 제한되지 않으며, 언급되지 않은 또 다른 기술적 과제들은 아래의 기재로부터 당업자에게 명확하게 이해될 수 있을 것이다.

과제의 해결 수단

[0006] 본 발명의 실시예에 따른 악성 사이트 차단 방법은 웹브라우저에 입력된 URL을 획득하는 단계, 상기 URL을 저장된 악성 사이트 패턴 목록과 비교하는 단계 및 상기 웹브라우저가 상기 URL로 이동하는 것을 차단하는 단계를 포함할 수 있다.

[0007] 실시예에서, 상기 URL을 획득하는 단계는 상기 URL의 도메인을 획득하는 단계를 포함할 수 있다.

[0008] 실시예에서, 상기 악성 사이트 패턴 목록을 획득하는 단계를 더 포함하고, 상기 악성 사이트 패턴 목록을 획득하는 단계는 APWG(Anti Phishing Working Group)으로부터 주기적으로 패턴 파일을 제공받는 단계 및 사용자들로부터 악성 사이트를 수집하는 단계중 적어도 어느 하나를 포함할 수 있다.

[0009] 실시예에서, 상기 악성 사이트 패턴 목록을 획득하는 단계는 상기 제공받은 패턴 파일 또는 상기 수집한 악성 사이트를 분석하여 URL을 분석하는 단계를 더 포함할 수 있다.

[0010] 실시예에서, 상기 차단하는 단계는 상기 URL이 상기 악성 사이트 패턴 목록에 포함되는 경우 사용자에게 차단 화면을 제공하는 단계 또는 상기 URL이 상기 악성 사이트 패턴 목록에 포함되지 않는 경우 웹브라우저가 상기 URL로 이동하는 단계 중 적어도 어느 하나를 포함할 수 있다.

[0011] 본 발명의 실시예에 따르면 악성 사이트 차단 방법을 컴퓨터에서 실행시키기 위한 프로그램을 기록한 컴퓨터가 읽을 수 있는 기록 매체일 수 있다.

[0012] 본 발명의 실시예에 따른 휴대 단말기는 표시부 및 제어부를 포함하고 상기 제어부는 웹브라우저에 URL이 입력되면 상기 웹브라우저가 URL로 이동하는 것을 차단하고, 상기 URL을 악성 사이트 패턴 목록과 비교하여 상기 URL이 상기 악성 사이트 패턴 목록에 포함되지 않은 경우, 상기 표시부가 상기 웹브라우저가 상기 URL로 이동한 결과를 제공하도록 제어할 수 있다.

[0013] 실시예에서, 상기 제어부는 상기 표시부에 다른 어플리케이션이 실행 중일 때는 백그라운드에서 서비스로써 동작할 수 있다.

[0014] 실시예에서, 상기 제어부는 APWG로부터 주기적으로 패턴 파일을 제공받거나 사용자들로부터 악성 사이트를 수집하여 상기 악성 사이트 패턴 목록을 획득할 수 있다.

[0015] 실시예에서, 상기 제어부는 획득한 상기 악성 사이트 패턴 목록을 분석하여 URL을 획득하고, 상기 입력된 URL이 상기 악성 사이트 패턴 목록에 포함되면 상기 표시부가 차단 화면을 제공하도록 제어할 수 있다.

발명의 효과

[0016] 본 발명의 일측면에 따르면, 금융 정보나 개인 정보를 탈취할 수 있는 악성 사이트 접근을 차단하여, 사용자의

정보를 보호할 수 있다.

[0017] 본 발명의 효과가 상술한 효과들로 한정되는 것은 아니며, 언급되지 아니한 효과들은 본 명세서 및 첨부된 도면들로부터 본 발명이 속하는 기술분야에서 통상의 지식을 가진 자에게 명확히 이해될 수 있을 것이다.

도면의 간단한 설명

[0018] 도 1은 본 발명의 실시예에 따른 악성 사이트 차단 방법을 설명하기 위한 도면이다.

도 2는 본 발명의 실시예에 따른 악성 사이트 패턴 목록을 획득하는 방법을 설명하기 위한 도면이다.

도 3은 본 발명의 실시예에 따른 재분류된 악성 사이트 패턴을 설명하기 위한 도면이다.

도 4는 본 발명의 실시예에 따른 안드로이드 플랫폼 기반의 휴대 단말기를 설명하기 위한 도면이다.

도 5 내지 도 7은 본 발명의 실시예에 따른 안드로이드 플랫폼 기반의 휴대 단말기의 동작을 설명하기 위한 도면이다.

발명을 실시하기 위한 구체적인 내용

[0019] 본 발명의 다른 이점 및 특징, 그리고 그것들을 달성하는 방법은 첨부되는 도면과 함께 상세하게 후술 되는 실시 예를 참조하면 명확해질 것이다. 그러나 본 발명은 이하에서 개시되는 실시 예에 한정되는 것이 아니라 서로 다른 다양한 형태로 구현될 수 있으며, 단지 본 실시 예는 본 발명의 개시가 완전하도록 하고, 본 발명이 속하는 기술분야에서 통상의 지식을 가진 자에게 발명의 범주를 완전하게 알려주기 위해 제공되는 것이며, 본 발명은 청구항의 범주에 의해 정의될 뿐이다.

[0020] 만일 정의되지 않더라도, 여기서 사용되는 모든 용어들(기술 혹은 과학 용어들을 포함)은 이 발명이 속한 종래 기술에서 보편적 기술에 의해 일반적으로 수용되는 것과 동일한 의미를 가진다. 일반적인 사전들에 의해 정의된 용어들은 관련된 기술 그리고/혹은 본 출원의 본문에 의미하는 것과 동일한 의미를 갖는 것으로 해석될 수 있고, 그리고 여기서 명확하게 정의된 표현이 아니더라도 개념화되거나 혹은 과도하게 형식적으로 해석되지 않을 것이다.

[0021] 본 명세서에서 사용된 용어는 실시 예들을 설명하기 위한 것이며 본 발명을 제한하고자 하는 것은 아니다. 본 명세서에서, 단수형은 문구에서 특별히 언급하지 않는 한 복수형도 포함한다. 명세서에서 사용되는 '포함한다' 및/또는 이 동사의 다양한 활용형들 예를 들어, '포함', '포함하는', '포함하고', '포함하며' 등은 언급된 조성, 성분, 구성요소, 단계, 동작 및/또는 소자는 하나 이상의 다른 조성, 성분, 구성요소, 단계, 동작 및/또는 소자의 존재 또는 추가를 배제하지 않는다.

[0022] 본 명세서에서 '및/또는' 이라는 용어는 나열된 구성들 각각 또는 이들의 다양한 조합을 가리킨다.

[0023] 한편, 본 명세서 전체에서 사용되는 '~부', '~기', '~블록', '~모듈' 등의 용어는 적어도 하나의 기능이나 동작을 처리하는 단위를 의미할 수 있다. 예를 들어 소프트웨어, FPGA 또는 ASIC과 같은 하드웨어 구성요소를 의미할 수 있다. 그렇지만 '~부', '~기', '~블록', '~모듈' 등이 소프트웨어 또는 하드웨어에 한정되는 의미는 아니다. '~부', '~기', '~블록', '~모듈'은 어드레싱할 수 있는 저장 매체에 있도록 구성될 수도 있고 하나 또는 그 이상의 프로세서들을 재생시키도록 구성될 수도 있다. 따라서, 일 예로서 '~부', '~기', '~블록', '~모듈'은 소프트웨어 구성요소들, 객체지향 소프트웨어 구성요소들, 클래스 구성요소들 및 태스크 구성요소들과 같은 구성요소들과, 프로세스들, 함수들, 속성들, 프로시저들, 서브루틴들, 프로그램 코드의 세그먼트들, 드라이버들, 펌웨어, 마이크로 코드, 회로, 데이터, 데이터베이스, 데이터 구조들, 테이블들, 어레이들 및 변수들을 포함한다. 구성요소들과 '~부', '~기', '~블록', '~모듈'들 안에서 제공되는 기능은 더 작은 수의 구성요소들 및 '~부', '~기', '~블록', '~모듈'들로 결합되거나 추가적인 구성요소들과 '~부', '~기', '~블록', '~모듈'들로 더 분리될 수 있다.

[0024] 본 발명은 안드로이드 플랫폼 기반의 휴대 단말기에서 피싱 사이트나 악성코드 배포사이트에서 배포된 악성 코드가 휴대 단말기에 설치되는 것을 방지하기 위해 악성 사이트로의 접근을 차단하는 방법에 관한 것이다. 실시예에 따르면, 악성 사이트로의 이동을 위해 웹브라우저에 URL이 입력되면, 입력된 URL을 분석하여 악성 사이트로의 이동을 차단할 수 있다. 이하 첨부된 도면을 참조하여 보다 상세히 설명할 것이다.

[0025] 도 1은 본 발명의 실시예에 따른 악성 사이트 차단 방법을 설명하기 위한 도면이다.

[0026] 도 1에 도시된 것처럼, 본 발명의 실시예에 따른 악성 사이트 차단 방법은 웹브라우저에 입력된 URL(Uniform Resource Locator)을 획득하는 단계(S10), 획득한 URL이 저장된 악성 사이트 목록에 존재하는지 비교하는 단계(S20) 및 비교 결과에 따라 웹브라우저가 URL로 이동하는 것을 차단하는 단계(S30)를 포함할 수 있다. 실시예에 따르면, 악성 사이트 차단 방법은 비교 결과에 따라 웹브라우저가 URL로 이동하는 단계(S40)를 더 포함할 수 있다.

[0027] 실시예에 따르면, 웹브라우저에 입력된 URL을 획득하는 단계(S10)는 획득한 URL의 도메인을 획득하는 단계(S12)를 포함할 수 있다. URL은 도메인과 서브 URL로 구성된다. 도메인은 인터넷상의 컴퓨터 주소를 알기 쉬운 영문으로 표현한 것으로, 시스템, 조직, 조직의 종류, 국가의 이름 순으로 구분되어 있다. 서브 URL은 도메인 뒤에 "/"로 구분되어 해당 도메인의 서브 페이지를 호출할 수 있게 해준다. 본 발명의 실시예에 따른 악성 사이트 차단 방법은 획득한 URL에서 도메인을 분리함으로써 도메인 레벨의 차단을 수행함과 동시에 악성 사이트 패턴 검색을 보다 효율적으로 할 수 있다.

[0028] 실시예에 따르면, 획득한 URL이 저장된 악성 사이트 패턴 목록에 존재하는지 비교하는 단계(S20)에서 악성 사이트 패턴 목록은 단말기에 미리 저장될 수 있고, 메모리에 미리 로드될 수 있다. 악성 사이트 패턴 목록을 획득하는 방법에 대해서는 도 2를 참조하여 보다 상세히 설명할 것이다.

[0029] 실시예에 따르면, 비교 결과에 따라 웹브라우저가 URL로 이동하는 것을 차단하는 단계(S30)는 사용자에게 차단 화면을 제공하는 단계(S32)를 포함할 수 있다. 사용자에게 차단 화면을 제공하는 단계(S32)는 URL이 악성 사이트 패턴 목록에 포함되는 경우, 미리 설정된 페이지로 리다이렉트하는 것에 의해 수행될 수 있다. 이와 동시에, 안드로이드 플랫폼이 설치된 단말기의 제어부는 사용자가 안드로이드 시스템의 백 버튼(back button)을 이용하여 차단된 페이지로 재방문하지 못하게 할 수 있다.

[0030] 실시예에 따르면, 비교 결과에 따라 웹브라우저가 URL로 이동하는 단계(S40)는 웹브라우저를 통해 URL의 내용을 사용자에게 제공함으로써 수행될 수 있다.

[0031] 도 2는 본 발명의 실시예에 따른 악성 사이트 패턴 목록을 획득하는 방법(S50)을 설명하기 위한 도면이다.

[0032] 도 2에 도시된 것처럼, 악성 사이트 패턴 목록을 획득하는 방법(S50)은 APWG(Anti Phishing Working Group)으로부터 주기적으로 패턴 파일을 제공받거나, 사용자들로부터 악성 사이트를 수집하는 단계(S52) 및 수집한 악성 사이트를 분석하여 URL을 재분류하는 단계(S54)를 포함할 수 있다.

[0033] 실시예에 따르면, 악성 사이트를 수집하는 단계(S52)는 안드로이드 플랫폼 기반의 휴대 단말기에 포함된 신고 기능을 통해 사용자의 동의 하에 수행될 수 있다. 이와 달리, APWG로부터 주기적으로 패턴 파일을 제공받아 수행될 수 있다. APWG는 예시적인 것으로, 악성 사이트를 수집하는 단계(S52)는 악성 사이트를 분석하는 다른 웹 페이지로부터 패턴 파일을 제공받아 수행될 수 있다.

[0034] 실시예에 따르면, 수집한 악성 사이트를 분석하여 URL을 재분류하는 단계(S54)는 안드로이드 플랫폼 기반의 휴대 단말기의 시스템의 패턴에 맞게 재분류하여 수행될 수 있다. 재분류된 URL의 패턴에 대해서는 도 3을 참조하여 보다 상세히 설명할 것이다.

[0035] 본 발명의 실시예에 따른 악성 사이트 패턴 목록을 획득하는 방법(S50)은 상술한 것처럼 안드로이드 플랫폼 기반의 휴대 단말기에서 수행될 수 있다. 이와 달리, 악성 사이트 패턴 목록을 획득하는 방법(S50)은 휴대 단말기와 무선 통신할 수 있는 업데이트 서버에 의해 수행될 수 있다. 실시예에 따르면, 업데이트 서버는 악성 사이트 패턴 목록을 안드로이드 플랫폼 기반의 휴대 단말기에 무선 통신을 이용하여 제공할 수 있다. 업데이트 서버는 안드로이드 플랫폼 기반의 휴대 단말기의 인증 절차를 거친 후 악성 사이트 패턴 목록을 제공할 수 있다. 악성 사이트 패턴 목록은 공개키 암호화를 사용하여 전자서명을 하고, 해쉬 알고리즘을 사용하여 무결성을 검사하며, HTTPS를 사용한 암호화 통신을 통해 안드로이드 플랫폼 기반의 휴대 단말기로 제공될 수 있다.

[0036] 도 3은 본 발명의 실시예에 따른 재분류된 악성 사이트 패턴을 설명하기 위한 도면이다.

[0037] 도 3에 도시된 바와 같이, 본 발명의 실시예에 따른 악성 사이트 패턴 목록은 하나의 악성 사이트 패턴 정보를 포함하는 다수의 라인을 포함할 수 있다. 실시예에 따르면, 악성 사이트 패턴은 브랜드명, 액션, 도메인명, 서브 URL, 웹브라우저 등의 항목을 포함할 수 있다. 상기 항목들은 예시적인 것들로, 악성 사이트 패턴은 필요에 따라 추가적으로 다른 항목을 더 포함할 수 있다. 실시예에 따르면, 상기 항목들은 구분자 "<? ?>"를 통해 구분될 수 있다. 상기 구분자는 예시적인 것으로 다른 문자도 구분자로 사용될 수 있다.

[0038] 실시예에 따르면, 상기 브랜드명은 패턴 목록에 저장된 패턴을 설명하기 위한 것으로 악성 사이트 패턴의 수집 경로, 악성 패턴이 사용되는 사이트 정보 등을 포함할 수 있다. 악성 사이트 패턴의 수집 경로 및 악성 패턴이 사용되는 사이트 정보 등은 예시적인 것이며, 악성 사이트 패턴을 설명하기 위한 다른 정보들을 포함하는 형태로 작성될 수 있다. 도 3에 도시된 "APWG EBAY"의 의미는 이 패턴이 APWG를 통해서 수집되었고 EBAY 사이트에서 사용되었던 패턴임을 의미한다. 도 3에 도시되지는 않았으나, 예를 들어 사용자가 신고한 악성 사이트 패턴으로 이 악성 사이트 패턴이 네이버에 사용되었으면 "USER NAVER"와 같이 작성될 수 있다.

[0039] 실시예에 따르면, 상기 액션은 상기 도메인에 대한 대응 방법을 포함할 수 있다. 예시적으로, 상기 액션은 상기 도메인을 완전 차단, 선택적 차단 혹은 허용하는 것일 수 있다. 완전 차단은 상기 도메인이 위험한 것으로 확인된 경우에 사용자의 접근을 자동으로 차단하여 수행될 수 있다. 선택적 차단은 상기 도메인의 위험 여부가 확실하지 않을 경우에 사용자에게 경고하고, 사용자의 책임에 의해 상기 도메인에 접속할 수 있도록 하여 수행될 수 있다. 허용은 상기 도메인이 안전한 것으로 확인된 경우에 상기 도메인에 자동으로 접속하여 수행될 수 있다.

[0040] 실시예에 따르면, 상기 액션은 약속된 숫자로 작성될 수 있으며, 각각의 숫자가 하나의 액션을 의미할 수 있다. 도 3에서는 "9"가 상기 도메인을 차단하는 것으로 표시되어 있으나, 사용자의 필요에 따라 다른 숫자 또는 문자 등으로 작성될 수 있다. 예시적으로, "9"는 완전 차단, "8"은 선택적 차단, "7"은 허용 등으로 작성될 수 있다.

[0041] 실시예에 따르면, 상기 도메인명은 피싱 사이트나 악성코드 배포사이트에 대한 도메인을 포함할 수 있다. 도 3에 도시된 것처럼, 상기 도메인명은 "duedaa.org"와 같은 도메인 네임이나, "111.90.133.28"와 같은 IP 주소, "adf.ly"와 같은 단축주소 등으로 작성될 수 있다. 실시예에 따르면, 피싱 사이트나 악성코드 배포사이트가 서브 URL을 포함하는 경우라도 도메인만을 따로 분리하여 패턴화 함으로써, 피싱 사이트나 악성코드 배포사이트를 포괄적으로 차단할 수 있다.

[0042] 실시예에 따르면, 상기 서브 URL은 피싱 사이트나 악성코드 배포사이트에 대한 서브 URL을 포함할 수 있다. 앞서 도메인명에서 설명한 것처럼, 피싱 사이트나 악성 코드 배포사이트가 서브 URL을 포함하더라도 도메인 레벨에서 차단할 수 있지만, 본 발명의 실시예에 따른 악성 사이트 패턴은 보다 정확하게 악성 사이트를 차단하기 위해 서브 URL을 더 포함할 수 있다.

[0043] 도 1에 도시된 획득한 URL이 저장된 악성 사이트 목록에 존재하는지 비교하는 단계(S20)는 획득한 URL의 도메인과 서브 URL을 악성 사이트 패턴 목록에 포함된 악성 사이트 패턴의 도메인명과 서브 URL을 각각 비교함으로써 수행될 수 있다.

[0044] 실시예에 따르면, 상기 웹브라우저 타입은 사용자의 웹브라우저 종류를 의미할 수 있다. 도 3에 도시된 것처럼, 웹브라우저 항목에 표시된 "[*]"는 모든 웹브라우저에 적용될 수 있는 악성 사이트 패턴임을 의미할 수 있다. 도 3에 도시되어 있지 않으나, 사용자가 사용하는 웹브라우저에 따라 상기 웹브라우저 타입은 익스플로러(Explorer), 사파리(Safari), 크롬(Chrome), 파이어폭스(Firefox) 등이 될 수 있다.

[0045] 도 4는 본 발명의 실시예에 따른 안드로이드 플랫폼 기반의 휴대 단말기를 설명하기 위한 도면이다.

[0046] 실시예에 따르면, 휴대 단말기는 사용자에게 어플리케이션의 동작을 제공하고 사용자로부터 터치 입력을 입력받을 수 있는 표시부와 휴대 단말기의 동작을 제어하는 제어부 및 악성 사이트 패턴 목록을 저장하는 저장부를 포함할 수 있다.

[0047] 실시예에 따르면, 제어부는 휴대 단말기의 웹브라우저에 URL이 입력되면 웹브라우저가 입력된 URL로 이동하는 것을 차단할 수 있다. 제어부는 입력된 URL을 도메인과 서브 URL로 구분하여 저장된 악성 사이트 패턴 목록과 비교하여 입력된 URL이 저장된 악성 사이트 패턴 목록에 포함되지 않은 경우에는 웹브라우저가 입력된 URL로 이동하도록 하고 표시부로 하여금 입력된 URL로 이동한 결과를 표시하도록 할 수 있다.

[0048] 실시예에 따르면, 제어부는 상기 동작을 다른 어플리케이션이 실행 중일 때 백그라운드에서 서비스로써 수행할

수 있다.

[0049] 실시예에 따르면, 제어부는 악성 사이트 패턴 목록을 APWG로부터 주기적으로 패턴 파일을 제공받아 획득하거나, 사용자들로부터 악성 사이트를 수집하여 획득할 수 있다. 이와 달리, 제어부는 악성 사이트 패턴 목록을 관리하는 업데이트 서버로부터 무선 통신을 통해 악성 사이트 패턴 목록을 획득할 수 있다.

[0050] 실시예에 따르면, 제어부는 입력된 URL이 저장된 악성 사이트 패턴 목록에 포함되면 표시부로 하여금 차단 화면을 제공하도록 제어할 수 있다.

[0051] 도 5 내지 도 7은 본 발명의 실시예에 따른 안드로이드 플랫폼 기반의 휴대 단말기의 동작을 설명하기 위한 도면이다.

[0052] 실시예에 따르면, 제어부는 다른 어플리케이션이 실행되지 않을 경우에는 도 5에 도시된 바와 같은 화면을 제공하도록 표시부를 제어할 수 있다. 제어부는 악성 사이트 패턴 목록을 미리 읽어 메모리에 로드함으로써, 악성 사이트 차단을 보다 빨리 수행할 수 있다.

[0053] 실시예에 따르면, 제어부는 도 5에 도시된 "LOG"가 터치되면, 표시부를 통해 사용자에게 동작 로그를 제공할 수 있다. 제어부는 "Add block url"이 터치되면, 사용자가 악성 사이트 패턴 목록에 차단할 악성 사이트를 추가하도록 할 수 있다. 제어부는 "Add allow url"이 터치되면, 사용자가 접속을 허용할 안전한 사이트를 추가하도록 할 수 있다. 사용자가 임의로 특정 사이트를 추가하는 경우, 제어부는 특정 사이트를 악성 사이트 패턴 목록에 추가적으로 저장할 수 있다.

[0054] 도 6 및 도 7은 본 발명의 실시예에 따른 휴대 단말기에서 웹브라우저에 URL이 입력된 경우를 설명하기 위한 도면이다. URL의 입력은 사용자가 직접 입력하여 수행되거나, 사용자가 웹브라우저 사용 중에 URL을 클릭하여 수행되거나, 사용자의 휴대 단말기로 수신된 문자 메세지에 포함된 URL을 클릭하여 수행될 수 있다.

[0055] 실시예에 따르면, 도 6에 도시된 바와 같이 웹브라우저에 URL이 입력되면 제어부는 입력된 URL을 획득할 수 있다. URL의 획득에 앞서, 제어부는 웹브라우저가 입력된 URL로 이동한 결과를 표시하기 전에 웹브라우저의 이동을 일시적으로 차단할 수 있다.

[0056] 다시 도 6을 참조하면, 웹브라우저의 이동이 차단된 동안 제어부는 "http://dlvr.it/3LJQwh"를 획득할 수 있다. 제어부는 획득한 URL에서 도메인인 "dlvr.it"와 서브 URL인 "/3LJQwh"를 분리하여 획득할 수 있다. 이후, 제어부는 획득한 도메인인 "dlvr.it"가 저장된 악성 사이트 패턴 목록에 있는지 비교할 수 있다.

[0057] 실시예에 따르면, "dlvr.it"가 저장된 악성 사이트 패턴 목록에 존재하지 않는 경우, 제어부는 웹브라우저의 이동 차단을 해제하고 입력된 URL로 웹브라우저를 이동시킨다. 이와 달리, "dlvr.it"가 저장된 악성 사이트 패턴 목록에 존재하는 경우, 제어부는 해당 악성 사이트 패턴의 액션에 따라 웹브라우저의 이동 차단을 유지하거나, 도 7에 도시된 바와 같이 차단 화면을 사용자에게 제공할 수 있다. 도 7에 도시된 차단 화면은 예시적인 것으로, 다른 차단 화면을 제공하거나 사용자 동의하에 위험을 감수하고 입력된 URL로 이동할 수 있게 하는 링크를 제공할 수 있다.

[0058] 아래 표 1 및 표 2는 본 발명의 실시예에 따른 안드로이드 플랫폼 기반의 휴대 단말기의 성능을 설명하기 위한 것이다.

[0059] 성능 테스트 있어서, 악성 사이트 패턴 목록에 포함된 악성 사이트 패턴의 수는 7272개였고, 웹브라우저에서 URL 입력되었을 때를 시작시간으로 하고, 차단이 완료되었을 때를 종료시간으로 하여 (종료시간-시작시간)을 차단시간으로 측정하였다. 테스트 기기 두 개에서 각각 10회씩 실행하여 차단 시간의 평균속도를 측정하였다. 표 1은 테스트 기기의 성능을 나타내고, 표 2는 차단 평균 속도를 나타내며 단위는 ms이다.

표 1

[0060]

모델명	SHV-E160S	Nexus-One
안드로이드 버전	4.1.2	2.3.6

인터넷 버전	4.1.2-E160SKSJMC4	2.3.6
CPU	15 GHz Dual-Core Qualcomm Snapdragon APQ8060	998 MHz Qualcomm Snapdragon QSD8250
GPU	Qualcomm Adreno 220	Qualcomm Adreno 200
RAM	1 GB	512 MB
ROM	16 GB	512 MB
제조사	Samsung Electronics	HTC Corporation

표 2

[0061]

	SHV-E160S	Nexus-One
1	293	15
2	465	14
3	183	13
4	199	14
5	195	9
6	147	12
7	138	12
8	158	16
9	149	17
10	159	10
평균	208.6	13.2

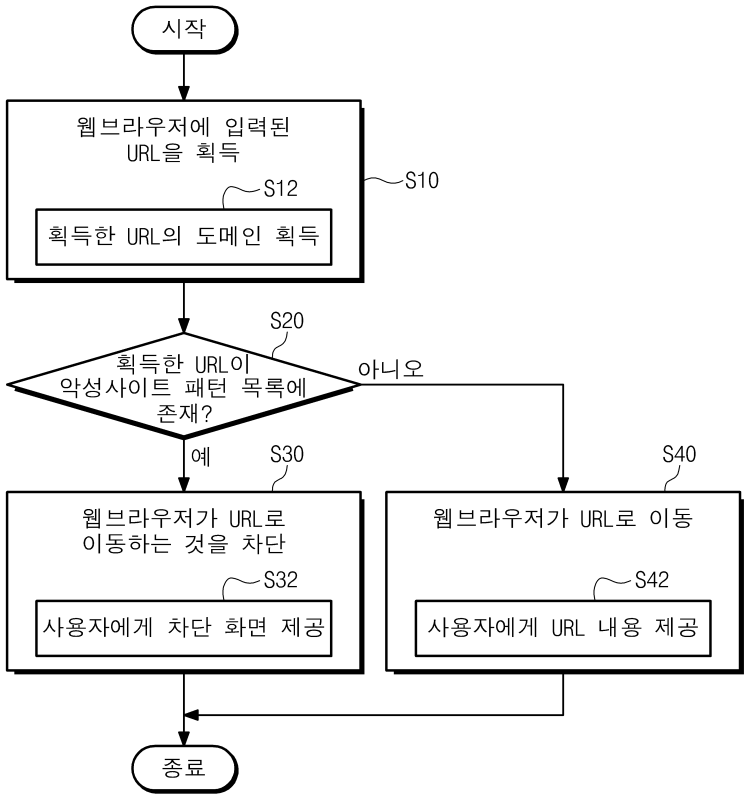
[0062] 표 2에서 보는 바와 같이 두 개의 테스트 기기에서 각각 평균 차단 속도는 208.6ms와 13.2ms로 상당히 빠른 속도로 차단됨을 알 수 있다.

[0063] 전술한 본 발명의 실시예에 따른 악성 사이트 차단 방법은 컴퓨터에서 실행되기 위한 프로그램으로 제작되어 컴퓨터가 읽을 수 있는 기록 매체에 저장될 수 있다. 상기 컴퓨터가 읽을 수 있는 기록 매체는 컴퓨터 시스템에 의하여 읽혀질 수 있는 데이터가 저장되는 모든 종류의 저장 장치를 포함한다. 컴퓨터가 읽을 수 있는 기록 매체의 예로는 ROM, RAM, CD-ROM, 자기 테이프, 플로피디스크, 광 데이터 저장 장치 등이 있다.

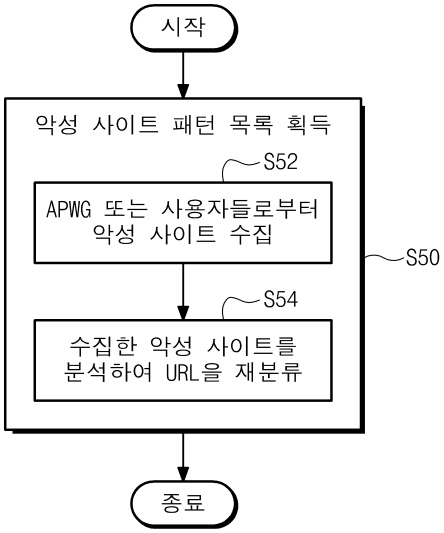
[0064] 이상의 실시예들은 본 발명의 이해를 돕기 위하여 제시된 것으로, 본 발명의 범위를 제한하지 않으며, 이로부터 다양한 변형 가능한 실시예들도 본 발명의 범위에 속할 수 있음을 이해하여야 한다. 예를 들어, 본 발명의 실시예에 도시된 각 구성 요소는 분산되어 실시될 수도 있으며, 반대로 여러 개로 분산된 구성 요소들은 결합되어 실시될 수 있다. 따라서, 본 발명의 기술적 보호범위는 특허청구범위의 기술적 사상에 의해 정해져야 할 것이며, 본 발명의 기술적 보호범위는 특허청구범위의 문언적 기재 그 자체로 한정되는 것이 아니라 실질적으로는 기술적 가치가 균등한 범주의 발명에 대하여까지 미치는 것임을 이해하여야 한다.

도면

도면1


시작
웹브라우저에 입력된 URL을 획득
S10
S12
획득한 URL의 도메인 획득
S20
획득한 URL이 악성사이트 패턴 목록에 존재?
아니오
예
S30
웹브라우저가 URL로 이동하는 것을 차단
S32
사용자에게 차단 화면 제공
S40
웹브라우저가 URL로 이동
S42
사용자에게 URL 내용 제공
종료

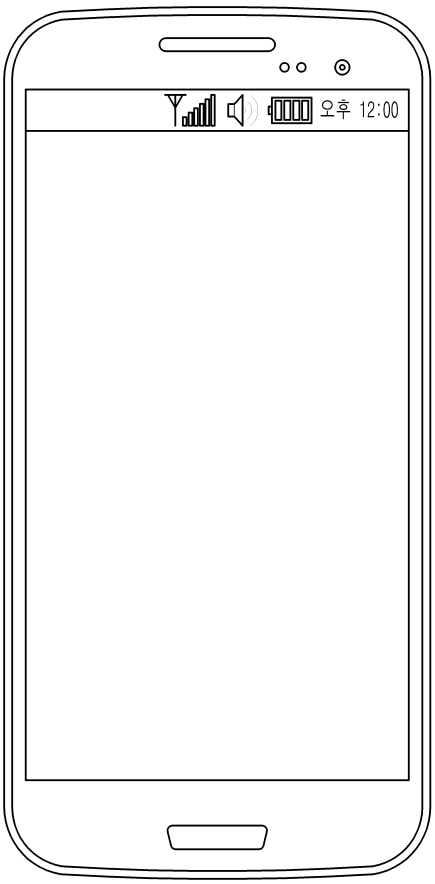
도면2


시작
악성 사이트 패턴 목록 획득
S50
S52
APWG 또는 사용자들로부터 악성 사이트 수집
S54
수집한 악성 사이트를 분석하여 URL을 재분류
종료

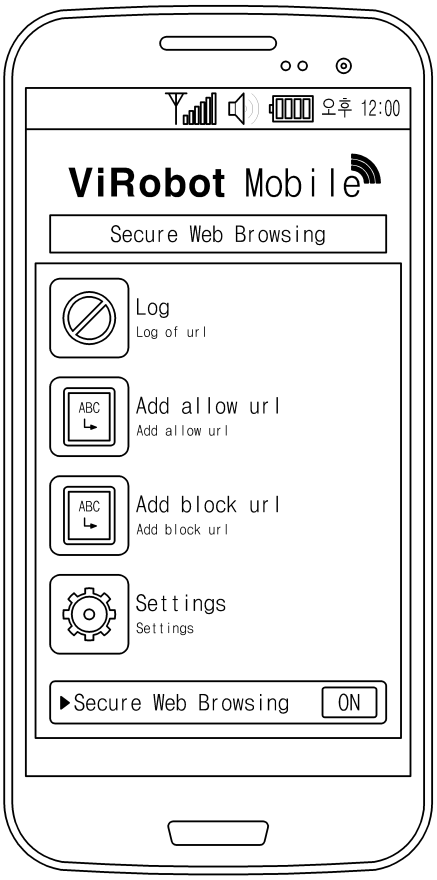
도면3

<?브랜드명?><?뱅샷?><?도메인명?><?서브URL?><?웹브라우저 타입?>
<?APWG EBAY?><?99?><?duedaa.org?><?/paypal/index.html?><?[*]?>
<?APWG EBAY?><?99?><?111.90.133.28?><?[*]?><?[*]?>
<?APWG EBAY?><?99?><?61w52c3xie.ssl.paypal-verifikation.org?><?/?><?[*]?>
<?APWG EBAY?><?99?><?adf.ly?><?/3106546/new?><?[*]?>

도면4



도면5


오후 12:00
ViRobot Mobile
Secure Web Browsing
Log
Log of url
Add allow url
Add allow url
Add block url
Add block url
Settings
Settings
▶Secure Web Browsing
ON

도면6


오후 12:00
http://dlvr.it/3LJQwh
Google 검색
이미지
로그인
Google
한글
?123
.com
이동

도면7