(19) 대한민국특허청(KR)
(12) 등록특허공보(B1)

(45) 공고일자 2015년09월01일
(11) 등록번호 10-1549342
(24) 등록일자 2015년08월26일

(51) 국제특허분류(Int. Cl.)
G06F 21/56 (2013.01)
(21) 출원번호 10-2014-0077831
(22) 출원일자 2014년06월25일
심사청구일자 2014년06월25일
(56) 선행기술조사문헌
KR1020100115182 A*
KR1020000012391 A
KR1020000030564 A
*는 심사관에 의하여 인용된 문헌

(73) 특허권자
고려대학교 산학협력단
서울특별시 성북구 안암로 145, 고려대학교 (안암동5가)
(72) 발명자
문종섭
서울특별시 동대문구 무학로42길 31 (제기동)
(74) 대리인
송인호, 민영준, 최관락

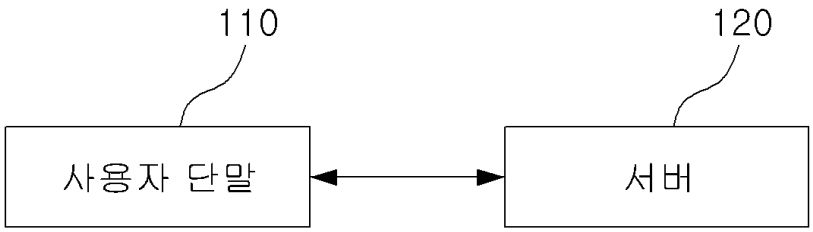
전체 청구항 수 : 총 6 항 심사관 : 구본재

(54) 발명의 명칭 **웹브라우저의 해킹을 방지하는 방법 및 그 장치**

(57) 요 약

웹브라우저의 해킹을 방지하는 방법 및 그 장치가 개시된다. 사용자 장치에서 웹 브라우저의 해킹을 방지하는 방법은, 상기 웹브라우저가 활성화된 상태에서 입력장치를 통해 입력되는 입력정보를 지정된 저장소에 저장하는 단계; 상기 웹브라우저를 통해 상기 입력정보가 표시된 상태에서 상기 웹브라우저를 통한 서버로의 제출 이벤트 발생을 감지하는 단계; 및 상기 제출 이벤트 발생이 감지되면, 상기 저장소에 저장된 입력정보를 이용하여 상기 웹브라우저로 입력된 입력정보 변경을 확인하여 해킹 여부를 판단하는 단계를 포함한다.

대 표 도 - 도1



특허청구의 범위

청구항 1

사용자 장치에서 웹 브라우저의 해킹을 방지하는 방법에 있어서,

상기 웹브라우저가 활성화된 상태에서 입력장치를 통해 입력되는 입력정보를 지정된 저장소에 저장하는 단계;

상기 웹브라우저를 통해 상기 입력정보가 표시된 상태에서 상기 웹브라우저를 통한 서버로의 제출 이벤트 발생을 감지하는 단계; 및

상기 제출 이벤트 발생이 감지되면, 상기 저장소에 저장된 입력정보를 이용하여 상기 웹브라우저로 입력된 입력정보 변경을 확인하여 해킹 여부를 판단하는 단계를 포함하되,

상기 해킹 여부를 판단하는 단계는,

상기 저장소에 저장된 입력정보와 상기 제출 이벤트 발생에 따라 상기 웹브라우저를 통해 전송되는 입력정보가 상이하면, 상기 제출 이벤트 발생 직후에 상기 웹브라우저에 입력된 입력정보가 해킹에 의해 변경된 것으로 판단하는 것을 특징으로 하는 웹브라우저 해킹 방지 방법.

청구항 2

삭제

청구항 3

제1 항에 있어서,

상기 해킹 여부를 판단한 결과 해킹으로 상기 웹브라우저로 입력된 입력정보가 변경된 것으로 판단되면, 상기 제출 이벤트 발생이 감지되더라도 상기 서버로 제출 요청을 전송하지 않는 단계를 더 포함하는 웹브라우저 해킹 방지 방법.

청구항 4

제1 항에 있어서,

상기 해킹 여부를 판단한 결과 해킹으로 상기 웹브라우저로 입력된 입력정보가 변경된 것으로 판단되면, 상기 서버로 해킹에 의한 입력정보 변경을 통지하거나 상기 사용자 장치를 통해 상기 입력정보 변경을 시청각 정보 형태로 표출시키는 단계를 더 포함하는 웹브라우저 해킹 방지 방법.

청구항 5

제1 항에 있어서,

상기 제출 이벤트 발생은 상기 웹브라우저를 통해 입력된 입력정보를 포함하는 인터넷 뱅킹 또는 온라인 거래를 위한 제출 또는 확인 명령의 선택에 의해 발생되는 것을 특징으로 하는 웹브라우저 해킹 방지 방법.

청구항 6

제1 항에 있어서,

상기 저장소는 상기 웹브라우저가 활성화된 상태에서 커널단에서 입력장치를 통해 입력되는 입력정보가 저장되는 논리적 저장영역이되,

상기 웹브라우저에 의해 접근이 불가능한 저장영역인 것을 특징으로 하는 웹브라우저 해킹 방지 방법.

청구항 7

입력부;

적어도 하나의 어플리케이션을 저장하는 메모리;

상기 메모리에 저장된 상기 어플리케이션을 실행하는 프로세서를 포함하되,

상기 프로세서에 의해 실행된 어플리케이션은,

웹브라우저가 활성화된 상태에서 상기 입력부를 통해 입력되는 입력정보를 저장소에 저장하는 단계;

상기 입력정보가 상기 웹브라우저를 통해 표시된 상태에서 상기 웹브라우저를 통한 서버로의 제출 이벤트 발생을 감지하는 단계; 및

상기 제출 이벤트 발생이 감지되면, 상기 저장소에 저장된 입력정보를 이용하여 상기 웹브라우저로의 입력정보 변경을 확인하여 해킹 여부를 판단하는 단계를 포함하되,

상기 해킹 여부를 판단하는 단계는,

상기 저장소에 저장된 입력정보와 상기 제출 이벤트 발생에 따라 상기 웹브라우저를 통해 전송되는 입력정보가 상이하면, 상기 제출 이벤트 발생 직후에 상기 웹브라우저에 입력된 입력정보가 해킹에 의해 변경된 것으로 판단하는 것을 특징으로 하는 사용자 장치.

명 세 서

기 술 분 야

[0001] 본 발명은 웹브라우저의 해킹을 방지하는 방법 및 그 장치에 관한 것이다.

배 경 기 술

[0002] 정보통신 기술의 발전으로 최근에는 인터넷 뱅킹을 통해 은행 업무를 대신하거나 온라인을 통해 상품을 구매하는 온라인 거래가 급속도로 증가하였다. 인터넷 뱅킹 또는 온라인 거래의 급증과 함께 최근에는 사회적으로 악성코드에 의한 해킹 문제가 크게 대두되고 있다.

[0003] 악성코드를 이용하여 웹브라우저를 해킹하는 경우, 사용자가 의도하지 않은 악성코드에 의해 지정된 엉뚱한 계좌로 악성코드에 의해 지정된 금액이 이체되어 사용자가 악성코드에 의한 웹브라우저 해킹을 인지하지 못하는 상태에서 거래가 이루어지게 된다. 따라서, 이러한 악의적인 웹브라우저 해킹을 방지하기 위한 다양한 방안에 대한 연구가 지속되어야 할 필요가 있다.

발명의 내용

해결하려는 과제

[0004] 본 발명은 사용자가 악의적인 악성코드에 의한 웹브라우저 해킹을 인지하지 못하는 상태에서 발생되는 웹브라우저 해킹을 방지할 수 있는 웹브라우저의 해킹을 방지하는 방법 및 그 장치를 제공하기 위한 것이다.

과제의 해결 수단

[0005] 본 발명의 일 측면에 따르면, 사용자가 악의적인 악성코드에 의한 웹브라우저 해킹을 인지하지 못하는 상태에서 발생되는 웹브라우저 해킹을 방지할 수 있는 방법 및 그 장치가 제공된다.

[0006] 본 발명의 일 실시예에 따르면, 사용자 장치에서 웹 브라우저의 해킹을 방지하는 방법에 있어서, 상기 웹브라우저가 활성화된 상태에서 입력장치를 통해 입력되는 입력정보를 지정된 저장소에 저장하는 단계; 상기 웹브라우저를 통해 상기 입력정보가 표시된 상태에서 상기 웹브라우저를 통한 서버로의 제출 이벤트 발생을 감지하는 단계; 및 상기 제출 이벤트 발생이 감지되면, 상기 저장소에 저장된 입력정보를 이용하여 상기 웹브라우저로 입력된 입력정보 변경을 확인하여 해킹 여부를 판단하는 단계를 포함하는 웹브라우저 해킹 방지 방법이 제공될 수 있다.

[0007] 상기 해킹 여부를 판단하는 단계는, 상기 저장소에 저장된 입력정보와 상기 제출 이벤트 발생에 따라 상기 웹브라우저를 통해 전송되는 입력정보가 상이하면, 상기 제출 이벤트 발생 직후에 상기 웹브라우저에 입력된 입력정보가 해킹에 의해 변경된 것으로 판단하는 단계를 포함할 수 있다.

[0008] 상기 해킹 여부를 판단한 결과 해킹으로 상기 웹브라우저로 입력된 입력정보가 변경된 것으로 판단되면, 상기 제출 이벤트 발생이 감지되더라도 상기 서버로 제출 요청을 전송하지 않는 단계를 더 포함할 수 있다.

[0009] 상기 해킹 여부를 판단한 결과 해킹으로 상기 웹브라우저로 입력된 입력정보가 변경된 것으로 판단되면, 상기 서버로 해킹에 의한 입력정보 변경을 통지하거나 상기 사용자 장치를 통해 상기 입력정보 변경을 시청각 정보 형태로 표출시키는 단계를 더 포함할 수 있다.

[0010] 상기 제출 이벤트 발생은 상기 웹브라우저를 통해 입력된 입력정보를 포함하는 인터넷 뱅킹 또는 온라인 거래를 위한 제출 또는 확인 명령의 선택에 의해 발생될 수 있다.

[0011] 상기 저장소는 상기 웹브라우저가 활성화된 상태에서 커널단에서 입력장치를 통해 입력되는 입력정보가 저장되는 논리적 저장영역이되, 상기 웹브라우저에 의해 접근이 불가능한 저장영역일 수 있다.

[0012] 본 발명의 다른 실시예에 따르면, 입력부; 적어도 하나의 어플리케이션을 저장하는 메모리; 상기 메모리에 저장된 상기 어플리케이션을 실행하는 프로세서를 포함하되, 상기 프로세서에 의해 실행된 어플리케이션은, 웹브라우저가 활성화된 상태에서 상기 입력부를 통해 입력되는 입력정보를 저장소에 저장하는 단계; 상기 입력정보가 상기 웹브라우저를 통해 표시된 상태에서 상기 웹브라우저를 통한 서버로의 제출 이벤트 발생을 감지하는 단계; 및 상기 제출 이벤트 발생이 감지되면, 상기 저장소에 저장된 입력정보를 이용하여 상기 웹브라우저로의 입력정보 변경을 확인하여 해킹 여부를 판단하는 단계를 포함하는 것을 특징으로 하는 사용자 장치가 제공될 수 있다.

발명의 효과

[0013] 본 발명의 일 실시예에 따른 웹브라우저의 해킹을 방지하는 방법 및 그 장치를 제공함으로써, 사용자가 악의적인 악성코드에 의한 웹브라우저 해킹을 인지하지 못하는 상태에서 발생되는 웹브라우저 해킹을 방지할 수 있다.

[0014] 이를 통해, 본 발명은 웹브라우저를 이용하여 사용자가 안심하고 인터넷 뱅킹이나 온라인 거래를 수행할 수 있도록 정상적인 인터넷 뱅킹 및 온라인 거래의 활성화를 지원할 수 있는 이점도 있다.

도면의 간단한 설명

[0015] 도 1은 본 발명의 일 실시예에 따른 웹브라우저의 해킹을 방지하기 위한 시스템 구성을 개략적으로 도시한 도면. .

도 2는 본 발명의 일 실시예에 따른 사용자 장치에서 웹브라우저의 해킹을 방지하는 방법을 나타낸 순서도.

도 3은 본 발명의 일 실시예에 따른 인터넷 뱅킹 화면을 도시한 도면.

도 4는 본 발명의 일 실시예에 따른 사용자 장치의 내부 구성을 개략적으로 도시한 블록도.

도 5는 본 발명의 다른 실시예에 따른 사용자 장치의 내부 구성을 개략적으로 도시한 블록도.

발명을 실시하기 위한 구체적인 내용

[0016] 본 발명은 다양한 변환을 가할 수 있고 여러 가지 실시예를 가질 수 있는 바, 특정 실시예들을 도면에 예시하고 상세한 설명에 상세하게 설명하고자 한다. 그러나, 이는 본 발명을 특정한 실시 형태에 대해 한정하려는 것이 아니며, 본 발명의 사상 및 기술 범위에 포함되는 모든 변환, 균등물 내지 대체물을 포함하는 것으로 이해되어야 한다. 본 발명을 설명함에 있어서 관련된 공지 기술에 대한 구체적인 설명이 본 발명의 요지를 흐릴 수 있다고 판단되는 경우 그 상세한 설명을 생략한다.

[0017] 제1, 제2 등의 용어는 다양한 구성요소들을 설명하는데 사용될 수 있지만, 상기 구성요소들은 상기 용어들에 의해 한정되어서는 안 된다. 상기 용어들은 하나의 구성요소를 다른 구성요소로부터 구별하는 목적으로만 사용된다.

[0018] 본 출원에서 사용한 용어는 단지 특정한 실시예를 설명하기 위해 사용된 것으로, 본 발명을 한정하려는 의도가 아니다. 단수의 표현은 문맥상 명백하게 다르게 뜻하지 않는 한, 복수의 표현을 포함한다. 본 출원에서, "포함하다" 또는 "가지다" 등의 용어는 명세서상에 기재된 특징, 숫자, 단계, 동작, 구성요소, 부품 또는 이들을 조합한 것이 존재함을 지정하려는 것이지, 하나 또는 그 이상의 다른 특징들이나 숫자, 단계, 동작, 구성요소, 부품 또는 이들을 조합한 것들의 존재 또는 부가 가능성을 미리 배제하지 않는 것으로 이해되어야 한다.

[0019] 도 1은 본 발명의 일 실시예에 따른 웹브라우저의 해킹을 방지하기 위한 시스템 구성을 개략적으로 도시한 도면이다.

[0020] 도 1을 참조하면, 본 발명의 일 실시예에 따른 웹브라우저의 해킹을 방지하기 위한 시스템은 사용자 장치(110)와 서버(120)로 구성된다.

[0021] 사용자 장치(110)는 웹브라우저가 설치되어 있으며, 웹브라우저를 통해 서버(120)와 연동되어 인터넷 뱅킹 또는 온라인 거래를 수행할 수 있는 장치이다.

[0022] 예를 들어, 사용자 장치(110)는 컴퓨터, 노트북, 이동통신 단말기 등일 수 있다.

[0023] 즉, 사용자 장치(110)는 웹브라우저가 설치되어 있으며, 통신 기능을 구비한 전자 장치인 경우 모두 동일하게 적용될 수 있다.

[0024] 또한, 사용자 장치(110)는 웹브라우저가 활성화된 상태에서 키보드, 터치패드, 터치스크린 등과 같은 입력장치를 통해 입력정보가 입력되는 경우, 입력정보가 웹브라우저의 유저인터페이스(DOM)로 전달되기 전에 커널단에서 입력정보를 수집하여 별도의 지정된 저장소에 저장할 수 있다.

[0025] 또한, 사용자 장치(110)는 웹브라우저의 제출 이벤트 발생 여부를 감지하고, 제출 이벤트 발생이 감지되면, 당해 저장소에 저장된 입력정보를 이용하여 웹브라우저의 해킹 여부를 판단하여 이를 제출 이벤트 발생에 상응하는 서버 또는 사용자에게 통지할 수 있다. 사용자 장치(110)는 웹브라우저가 활성화된 상태에서 인터넷 뱅킹 또는 온라인 거래에 상응하는 제출 또는 확인 메뉴가 입력 장치를 통해 선택되면, 당해 웹브라우저에 제출 이벤트가 발생한 것으로 인식할 수 있다. 즉, 웹브라우저는 인터넷 뱅킹 또는 온라인 거래에 상응하여 사용자로부터 제출 또는 확인 메뉴가 선택되면 제출 이벤트가 발생한 것으로 인식할 수 있다.

[0026] 이에 따라, 일반적인 인터넷 뱅킹 또는 온라인 거래의 경우 웹브라우저는 사용자에 의해 입력장치를 통해 입력되어 당해 웹브라우저를 통해 화면에 표시된 입력정보를 포함하여 서버로 인터넷 뱅킹 또는 온라인 거래를 요청하게 된다.

[0027] 그러나, 본 발명의 일 실시예에서는 사용자 장치(110)가 웹브라우저의 제출 이벤트 발생이 감지되면, 당해 웹브라우저로의 입력된 입력값의 변경여부를 확인하여 웹브라우저 해킹 여부를 판단할 수 있다. 즉, 사용자 장치(110)는 웹브라우저의 제출 이벤트 발생이 감지되면, 저장소에 저장된 입력정보를 이용하여 웹브라우저로 입력된 입력정보의 입력값 변경 여부를 확인할 수 있다. 이미 전술한 바와 같이, 저장소에 저장된 입력정보는 웹브라우저로 입력정보가 전달되기 이전에 커널단에서 수집되어 저장된 입력정보로 악성코드를 이용하여 웹브라우저를 후킹 또는 해킹하는 경우 웹브라우저로 입력된 입력정보와는 일치하지 않게된다. 이로 인해, 사용자 장치(110)는 저장소에 저장된 입력정보를 이용하여 웹브라우저의 해킹 여부를 판단할 수 있다.

[0028] 사용자 장치(110)에서 웹브라우저의 해킹을 판단하는 방법에 대해서는 이하 도 2에서 보다 상세히 설명하기로 한다.

[0029] 서버(120)는 당해 사용자 장치(110)로 인터넷 뱅킹 또는 온라인 거래를 위한 웹페이지를 제공하고, 사용자 장치(110)의 인터넷 뱅킹 또는 온라인 거래 요청에 따른 인터넷 뱅킹 또는 온라인 거래를 제공하기 위한 기능을 한다. 서버(120)에서 인터넷 뱅킹 또는 온라인 거래를 위한 웹페이지를 제공하고, 인터넷 뱅킹 또는 온라인 거래에 필요한 관련 정보를 제공받아 인터넷 뱅킹 또는 온라인 거래를 제공하는 자체는 이미 당업자에게는 자명한 사항이므로 이에 대한 별도의 설명은 생략하기로 한다.

[0030] 또한, 도 1에는 별도로 도시되어 있지 않으나, 서버(120)는 사용자 장치(110)의 인증정보를 인정하기 위한 별도의 인증서버와 연동되어 있을 수도 있음은 자명하다.

[0031] 도 2는 본 발명의 일 실시예에 따른 사용자 장치에서 웹브라우저의 해킹을 방지하는 방법을 나타낸 순서도이고, 도 3은 본 발명의 일 실시예에 따른 인터넷 뱅킹 화면을 도시한 도면이다. 이하에서는 이해와 설명의 편의를 도모하기 위해, 사용자 장치(110)는 서버(120)와 연동되어 인터넷 뱅킹 또는 온라인 거래를 위한 웹 페이지를 수신한 이후의 과정에 대해 설명하기로 한다. 또한, 이하에서는 이해와 설명의 편의를 도모하기 위해 사용자 장치(110)가 은행, 증권사 등의 서버(120)에 연결되어 인터넷 뱅킹을 진행하는 것을 가정하여 설명하기로 한다.

[0032] 인터넷 뱅킹을 위해 사전에 사용자 장치(110)는 웹페이지를 렌더링하여 표시할 수 있는 웹브라우저가 설치되어 있으며, 해당 웹브라우저가 실행되어 있는 것을 가정하기로 한다.

[0033] 단계 210에서 사용자 장치(110)는 실행된 웹페이지를 통해 서버(120)에 접속하여 인터넷 뱅킹을 위한 웹 페이지를 요청하고, 서버(120)로부터 해당 요청에 따른 웹페이지를 수신한 후 렌더링하여 인터넷 뱅킹 화면을 표시한

다.

[0034] 단계 215에서 사용자 장치(110)는 사용자로부터 입력장치를 통해 입력정보를 입력받는다. 이때, 사용자 장치(110)상에는 인터넷 뱅킹 화면이 표시된 웹브라우저가 활성화된 상태일 수 있다.

[0035] 단계 220에서 사용자 장치(110)는 인터넷 뱅킹 화면이 표시된 웹브라우저가 활성화된 상태에서 입력장치를 통해 입력된 입력정보를 지정된 별도의 저장소에 저장함과 동시에 웹브라우저의 유저인터페이스(DOM)로 전달한다.

[0036] 즉, 키보드, 터치 패드 등과 같은 입력장치를 통해 사용자로부터 필요한 정보가 입력되는 경우, 입력장치의 입력버퍼에 일시적으로 저장된 입력정보는 웹브라우저의 유저인터페이스(DOM)로 전달될 수 있다.

[0037] 이와 함께, 사용자 장치(110)는 입력장치의 입력버퍼에 일시적으로 저장된 입력정보를 커널단에서 획득하고, 이를 지정된 별도의 저장소에 저장할 수 있다. 여기서, 저장소는 논리적 저장영역으로 커널단에서 입력장치를 통해 입력되는 정보를 저장할 수 있는 저장공간이다.

[0038] 단계 225에서 사용자 장치(110)는 웹브라우저를 통한 제출 이벤트가 발생되었는지 여부를 판단한다.

[0039] 예를 들어, 사용자가 도 3과 같이, 인터넷 뱅킹 화면이 표시된 웹브라우저를 통해 인터넷 뱅킹을 위해 필요한 다양한 정보가 모두 입력된 이후, 제출 또는 이체와 같은 메뉴버튼이 선택되는 경우, 사용자 장치(110)는 웹브라우저를 통한 제출 이벤트가 발생한 것으로 인식할 수 있다.

[0040] 만일 제출 이벤트 발생이 감지되지 않은 경우, 단계 225에서 대기한다.

[0041] 따라서, 만일 제출 이벤트 발생이 감지되면(즉, 제출 이벤트가 발생되면), 단계 230에서 사용자 장치(110)는 저장소에 저장된 입력정보를 이용하여 웹브라우저의 해킹 여부를 판단한다.

[0042] 예를 들어, 사용자 장치(110)는 저장소에 저장된 입력정보와 제출 이벤트 발생에 따른 웹브라우저의 메모리에 저장된 입력정보가 일치하는지를 확인하여 웹브라우저의 해킹 여부를 판단할 수 있다.

[0043] 인터넷 뱅킹을 이용하는 경우, 악성코드는 일반적으로 사용자가 웹브라우저를 통해 인터넷 뱅킹 이체 확인을 위한 메뉴버튼이 선택되는 경우(즉, 제출 이벤트가 발생하는 경우) 제출 이벤트 발생 직후에 사용자에 의해 입력된 입력정보를 다른 입력정보로 대체하여 엉뚱한 금액이 엉뚱한 계좌로 이체되도록 할 수 있다.

[0044] 따라서, 본 발명의 일 실시예에서는 사용자 장치(110)가 웹브라우저를 통해 인터넷 뱅킹 또는 온라인 거래를 위한 제출 이벤트가 발생되면, 입력장치의 입력정보를 저장하는 별도의 저장소에 저장된 입력정보와 제출 이벤트 발생에 따라 서버(120)로 전송될 입력정보간의 일치 여부를 확인하여 웹브라우저의 해킹에 의한 피해를 방지하도록 할 수 있는 이점이 있다.

[0045] 만일 웹브라우저가 해킹된 것으로 판단되면, 단계 235에서 사용자 장치(110)는 웹브라우저의 제출 이벤트가 발생되었더라도 서버(120)로 인터넷 뱅킹 또는 온라인 거래를 요청하지 않는다. 즉, 웹브라우저가 해킹된 것으로 판단되면, 사용자 장치(110)는 웹브라우저의 제출 이벤트 발생에도 불구하고 서버(120)로 웹브라우저의 해킹 여부를 통지하거나 사용자에게 이를 알리도록 메시지를 표출시킬수 있다.

[0046] 그러나 만일 웹브라우저 해킹되지 않은 경우, 단계 240에서 사용자 장치(110)는 웹브라우저의 제출 이벤트 발생에 상응하여 정상적으로 입력정보를 포함하는 인터넷 뱅킹 또는 온라인 거래를 서버(120)로 요청한다.

[0047] 도 4는 본 발명의 일 실시예에 따른 사용자 장치의 내부 구성을 개략적으로 도시한 블록도이다.

[0048] 도 4를 참조하면, 본 발명의 일 실시예에 따른 사용자 장치(110)는 통신부(410), 입력부(415), 디스플레이부(420), 메모리(425) 및 프로세서(430)를 포함한다.

[0049] 통신부(410)는 서버(120)와 통신 연결되어 데이터를 송수신하는 기능을 한다. 예를 들어, 통신부(410)는 서버(120)를 통해 인터넷 뱅킹 또는 온라인 거래를 위한 웹페이지를 수신할 수 있다.

[0050] 입력부(415)는 당해 사용자 장치(110)을 제어하기 위한 다양한 제어 명령, 어플리케이션을 실행 또는 제어하기 위한 명령, 데이터 등을 입력받기 위한 수단이다. 예를 들어, 입력부(415)는 키보드, 터치패드, 키버튼 형식으로 구현될 수 있다.

[0051] 디스플레이부(420)는 다양한 데이터를 시각 정보의 형태로 출력하는 기능을 한다. 예를 들어, 디스플레이부(420)는 웹브라우저에 의해 렌더링된 화면을 출력할 수 있다. 예를 들어, 디스플레이부(420)는 액정화면일 수

있다.

[0052] 메모리(425)는 본 발명의 일 실시예에 따른 웹브라우저 해킹을 방지하기 위해 필요한 다양한 어플리케이션을 저장한다.

[0053] 프로세서(430)는 본 발명의 일 실시예에 따른 사용자 장치(110)의 내부 구성 요소들(예를 들어, 통신부(410), 입력부(415), 메모리(425) 등)을 제어하는 기능을 수행한다.

[0054] 또한, 프로세서(430)는 메모리(425)와 연동되어 해당 메모리(425)에 저장된 어플리케이션을 실행할 수 있다. 프로세서(430)에 의해 실행된 어플리케이션은 도 2에서 설명한 바와 같이 인터넷 뱅킹 또는 온라인 거래에 따른 웹브라우저 해킹을 방지하기 위한 일련의 단계를 수행할 수 있다. 이는 이미 도 2에서 설명한 바와 동일하므로 중복되는 설명은 생략하기로 한다.

[0055] 도 5는 본 발명의 다른 실시예에 따른 사용자 장치의 내부 구성을 개략적으로 도시한 블록도이다.

[0056] 도 5를 참조하면, 본 발명의 일 실시예에 따른 사용자 장치(110)는 통신부(510), 입력부(515), 수집부(520), 탐지부(525), 디스플레이부(530), 메모리(535) 및 프로세서(540)를 포함하여 구성된다.

[0057] 여기서, 통신부(510), 입력부(515), 디스플레이부(530), 메모리(535) 및 프로세서(540)의 기본 구성은 도 4에서 설명한 바와 동일하므로 중복되는 설명은 생략하기로 하며 상이한 구성에 대해서만 설명하기로 한다.

[0058] 수집부(520)는 프로세서(540)의 제어에 따라 웹브라우저가 활성화된 상태에서 입력부(515)를 통해 입력되는 입력정보를 수집하여 별도의 저장소에 저장하는 기능을 한다. 여기서, 별도의 저장소는 이미 전술한 바와 같이, 커널단에서 입력부(515)를 통해 입력되는 입력정보만을 수집하여 저장하는 논리적 저장 공간으로 웹브라우저를 비롯한 다른 일반적인 어플리케이션에 의해 접근이 불가능한 저장 공간일 수 있다.

[0059] 탐지부(525)는 인터넷 뱅킹 또는 온라인 거래를 위해 웹브라우저가 활성화된 상태에서 웹브라우저의 해킹 여부를 탐지하는 기능을 한다.

[0060] 예를 들어, 탐지부(525)는 인터넷 뱅킹 또는 온라인 거래를 위한 웹브라우저의 제출 이벤트 발생 여부를 감지하고, 제출 이벤트 발생 감지시 저장소에 저장된 입력정보를 이용하여 웹브라우저의 해킹 여부를 판단할 수 있다. 즉, 탐지부(525)는 저장소에 저장된 입력정보와 제출 이벤트 발생에 따른 웹브라우저의 메모리에 저장된 입력정보가 일치하는지를 확인하여 웹브라우저의 해킹 여부를 판단할 수 있다. 이는 도 2에서 설명한 바와 동일하므로 중복되는 설명은 생략하기로 한다.

[0061] 탐지부(525)에 의해 웹브라우저가 해킹된 것으로 판단되면, 프로세서(540)는 웹브라우저에서의 제출 이벤트 발생에도 불구하고 인터넷 뱅킹 또는 온라인 거래 요청을 서버(120)로 전송하지 않고, 웹브라우저 해킹을 서버(120)로 통지하거나 사용자에게 이를 통지할 수 있다.

[0062] 상기에서는 본 발명의 바람직한 실시예를 참조하여 설명하였지만, 해당 기술 분야에서 통상의 지식을 가진 자라면 하기의 특허 청구의 범위에 기재된 본 발명의 사상 및 영역으로부터 벗어나지 않는 범위 내에서 본 발명을 다양하게 수정 및 변경시킬 수 있음을 이해할 수 있을 것이다.

부호의 설명

[0063] 510: 통신부

515: 입력부

520: 수집부

525: 탐지부

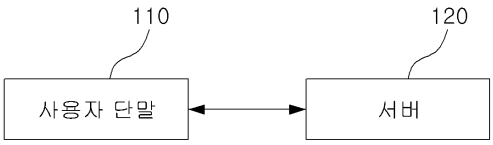
530: 디스플레이부

535: 메모리

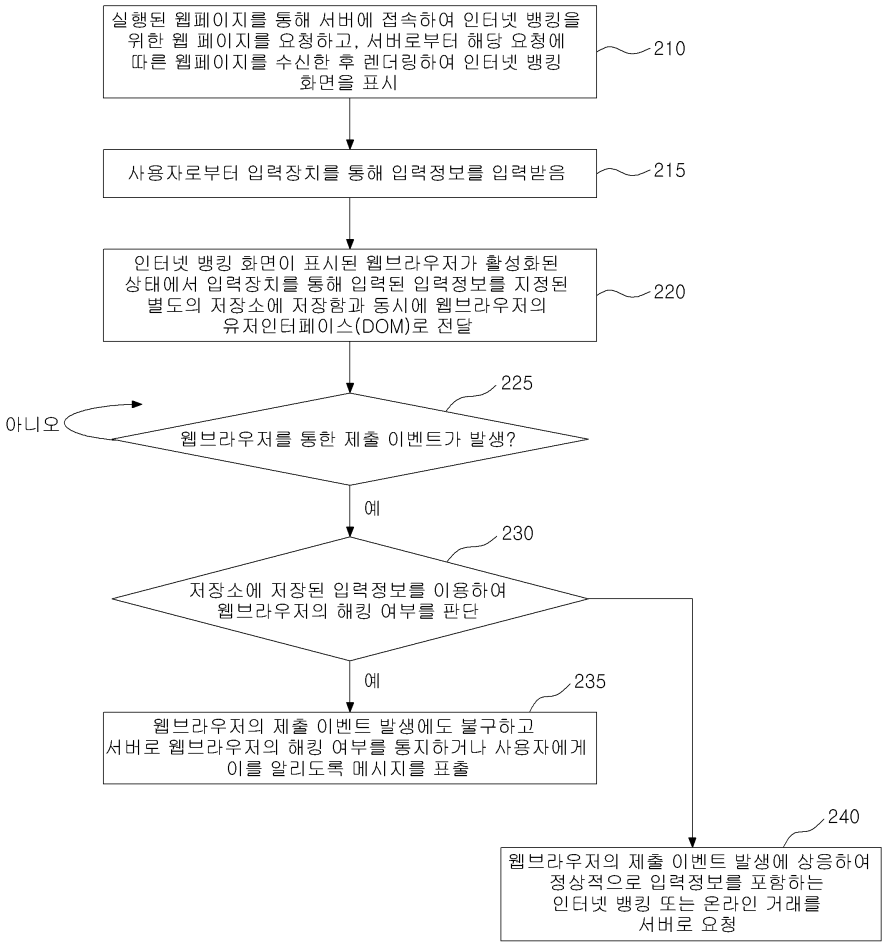
540: 프로세서

도면

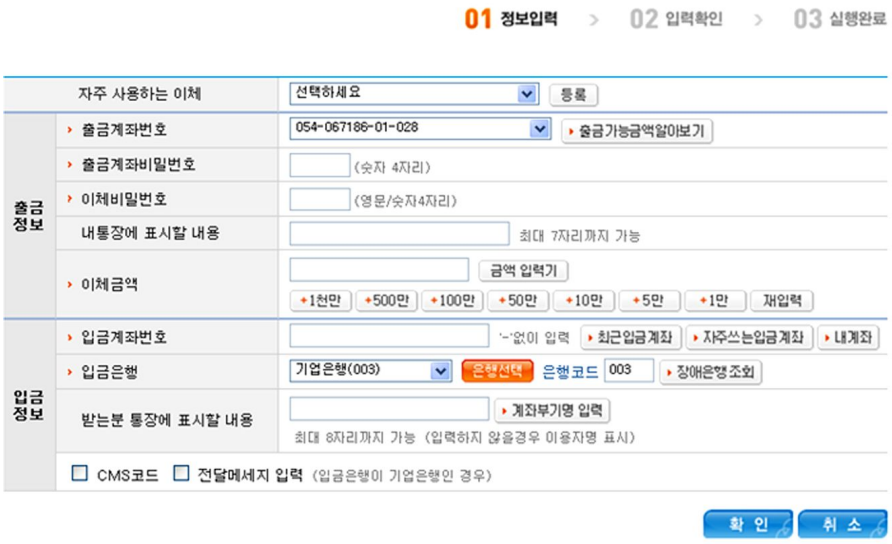
도면1


110
120
사용자 단말
서버

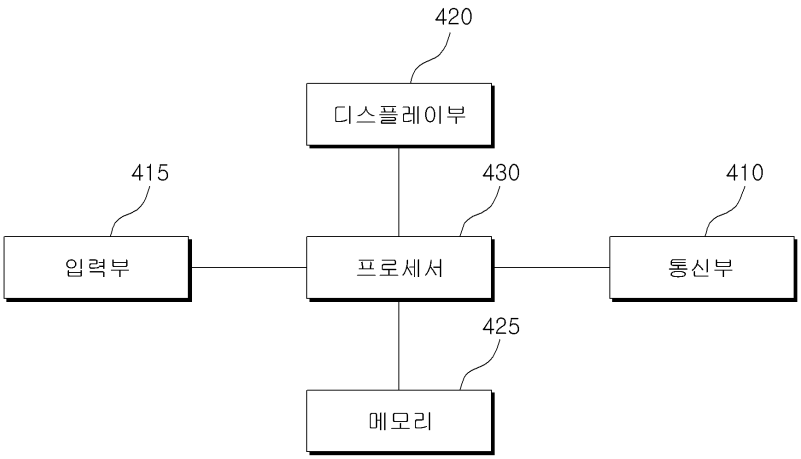
도면2


실행된 웹페이지를 통해 서버에 접속하여 인터넷 뱅킹을 위한 웹 페이지를 요청하고, 서버로부터 해당 요청에 따른 웹페이지를 수신한 후 렌더링하여 인터넷 뱅킹 화면을 표시
210
사용자로부터 입력장치를 통해 입력정보를 입력받음
215
인터넷 뱅킹 화면이 표시된 웹브라우저가 활성화된 상태에서 입력장치를 통해 입력된 입력정보를 지정된 별도의 저장소에 저장함과 동시에 웹브라우저의 유저인터페이스(DOM)로 전달
220
225
웹브라우저를 통한 제출 이벤트가 발생?
아니오
예
230
저장소에 저장된 입력정보를 이용하여 웹브라우저의 해킹 여부를 판단
예
235
웹브라우저의 제출 이벤트 발생에도 불구하고 서버로 웹브라우저의 해킹 여부를 통지하거나 사용자에게 이를 알리도록 메시지를 표출
240
웹브라우저의 제출 이벤트 발생에 상응하여 정상적으로 입력정보를 포함하는 인터넷 뱅킹 또는 온라인 거래를 서버로 요청

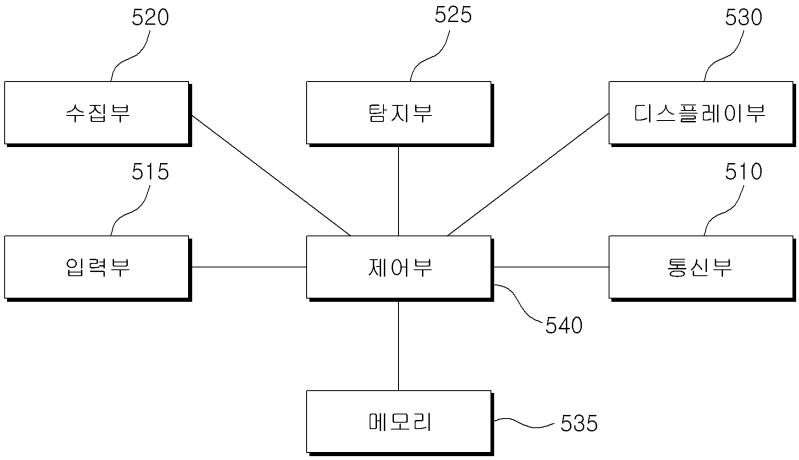
도면3


01 정보입력
02 입력확인
03 실행완료
자주 사용하는 이체
선택하세요
등록
출금 정보
출금계좌번호
054-067186-01-028
출금가능금액알아보기
출금계좌비밀번호
(숫자 4자리)
이체비밀번호
(영문/숫자4자리)
내통장에 표시할 내용
최대 7자리까지 가능
이체금액
금액 입력기
+1천만
+500만
+100만
+50만
+10만
+5만
+1만
재입력
입금 정보
입금계좌번호
'-'없이 입력
최근입금계좌
자주쓰는입금계좌
내계좌
입금은행
기업은행(003)
은행선택
은행코드
003
장애은행조회
받는분 통장에 표시할 내용
계좌부기명 입력
최대 8자리까지 가능 (입력하지 않을경우 이용자명 표시)
CMS코드
전달메세지 입력
(입금은행이 기업은행인 경우)
확 인
취 소

도면4


420
디스플레이부
415
430
410
입력부
프로세서
통신부
425
메모리

도면5


520
525
530
수집부
탐지부
디스플레이부
515
510
입력부
제어부
통신부
540
메모리
535