(19) 대한민국특허청(KR)
(12) 등록특허공보(B1)

(45) 공고일자 2014년02월06일
(11) 등록번호 10-1358565
(24) 등록일자 2014년01월27일

(51) 국제특허분류(Int. Cl.)
H04L 9/32 (2006.01) *H04W 12/06* (2009.01)
H04W 4/02 (2009.01)
(21) 출원번호 10-2012-0091610
(22) 출원일자 2012년08월22일
심사청구일자 2012년08월22일
(56) 선행기술조사문헌
KR1020030031087 A*
KR1020120069401 A*
KR1020120084630 A*
*는 심사관에 의하여 인용된 문헌

(73) 특허권자
인하대학교 산학협력단
인천광역시 남구 인하로 100, 인하대학교 (용현동)
(72) 발명자
양대헌
서울 서초구 서초중앙로 200, 13동 1407호 (서초동, 삼풍아파트)
(74) 대리인
양성보

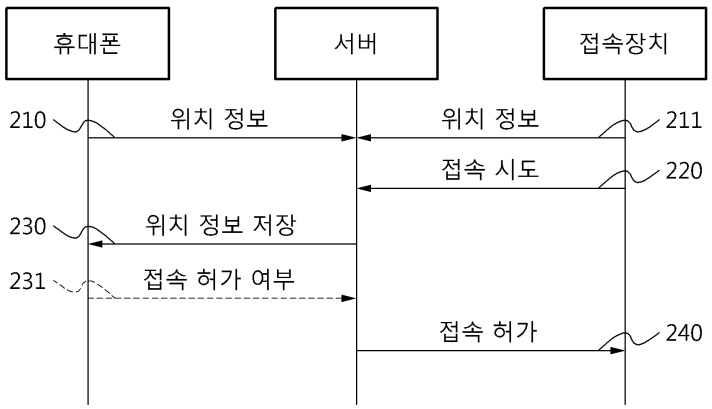
전체 청구항 수 : 총 6 항 심사관 : 홍기완

(54) 발명의 명칭 **접속장치와 휴대폰의 지리적 거리 차이를 이용한 접속장치 인증 방법 및 시스템**

(57) 요 약

본 발명은 피싱(Phishing) 공격을 방어하기 위한 것으로, 자세히는 접속장치와 휴대폰의 위치 정보를 이용한 방법 및 그 시스템에 관한 것이다. 접속장치 인증 방법에 있어서, 서버에서 사용자의 휴대폰과 접속장치의 위치 정보를 수신하는 단계; 서버는 상기 접속장치로부터의 접속 시도를 식별하고, 휴대폰으로 접속장치의 위치 정보를 전송하는 단계; 및 서버는 미리 정해진 식별자를 이용한 상기 접속장치의 접속을 허용하는 단계를 포함하는 접속장치 인증 방법이 제공될 수 있다.

대 표 도 - 도2



특허청구의 범위

청구항 1

접속장치 인증 방법에 있어서,

서버에서 사용자의 휴대폰과 접속장치의 위치 정보를 수신하는 단계;

상기 서버는 상기 접속장치로부터의 접속 시도를 식별하는 단계;

상기 접속장치의 IP 주소 또는 MAC 주소가 상기 접속장치의 위치 정보로서 미리 등록되었는지 여부를 확인하는 단계;

상기 접속장치의 IP 주소 또는 MAC 주소가 상기 접속장치의 위치 정보로서 미리 등록된 경우, 상기 휴대폰으로부터 접속 허가가 있었는지 여부와 무관하게 상기 접속 장치의 접속을 허용하고, 상기 접속장치의 IP 주소 또는 MAC 주소가 상기 접속장치의 위치 정보로서 미리 등록되어 있지 않은 경우, 상기 휴대폰으로 상기 접속장치의 위치 정보를 전송하는 단계; 및

상기 서버는 상기 휴대폰으로부터 접속 허가가 있는 경우에만 상기 접속 정차의 접속 시도를 허용하는 단계

를 포함하고,

상기 위치 정보를 전송하는 시기는 사용자에 의해 선택되는 것이며,

상기 접속장치의 위치 정보를 전송하는 단계는,

상기 접속장치의 위치 정보와 함께 상기 휴대폰으로 문자열 또는 그림을 전송하고,

상기 휴대폰과 상기 접속장치의 거리 차이가 일정 거리 미만이라면, 상기 위치 정보와 함께 상기 서버로의 접속이 위험하지 않다는 신호를 상기 휴대폰으로 전송하며,

상기 휴대폰과 상기 접속장치의 거리 차이가 일정 거리 이상이라면, 상기 위치 정보와 함께 상기 서버로의 접속이 위험하다는 경고 신호를 상기 휴대폰으로 전송하는 것인 접속장치 인증 방법.

청구항 2

제1항에 있어서,

상기 서버에서 사용자의 휴대폰과 상기 접속장치의 위치 정보를 수신하는 단계에서 획득하는 상기 위치 정보는

지피에스(GPS; Global Positioning System), 아이피 주소(IP Address; Internet Protocol Address), 맥 주소(MAC Address; Media Access Control Address) 중 적어도 하나를 이용하여 획득하는 것

을 특징으로 하는 접속장치 인증 방법.

청구항 3

제1항에 있어서,

상기 접속장치의 위치 정보를 전송하는 단계는

푸시(Push) 알림, 문자 메시지 또는 음성 알림 중 적어도 하나의 방법으로 위치 정보를 휴대폰으로 전송하는 것

을 특징으로 하는 접속장치 인증 방법.

청구항 4

삭제

청구항 5

제1항에 있어서,

상기 서버에서 사용자의 휴대폰과 상기 접속장치의 위치 정보를 수신하는 단계에서 획득하는 상기 위치 정보는,

상기 휴대폰과 상기 접속장치의 거리 차이를 포함하는 것

을 특징으로 하는 접속장치 인증 방법.

청구항 6

삭제

청구항 7

제1항에 있어서,

상기 접속장치의 접속을 허용하는 단계는

상기 휴대폰과 상기 접속장치의 거리 차이가 일정 거리 미만이라면, 상기 접속장치의 접속을 허가하며,

상기 휴대폰과 상기 접속장치의 거리 차이가 일정 거리 이상이라면, 상기 접속장치의 접속을 허가하지 않는 것

을 특징으로 하는 접속장치 인증 방법.

청구항 8

제1항에 있어서,

상기 접속장치의 접속을 허용하는 단계는

상기 서버가 상기 휴대폰으로부터 접속 허용 여부에 대한 메시지를 수신하는 것

을 특징으로 하는 접속장치 인증 방법.

청구항 9

삭제

청구항 10

삭제

명 세 서

기 술 분 야

[0001] 본 발명은 피싱(Phishing) 공격을 방어하기 위한 것으로, 자세히는 접속장치와 휴대폰의 위치 정보를 이용한 방법 및 그 시스템에 관한 것이다.

배 경 기 술

[0002] 단순한 피싱 방법으로는 공식사이트와 비슷한 모양의 웹 페이지를 보여주고 사용자에게 인터넷 뱅킹에 필요한 모든 정보를 입력하도록 요구하는 단순한 형태의 피싱(Phishing) 사이트가 등장했다.

[0003] 하지만, 다음의 두 가지 이유로 더 이상 쉽게 피싱 공격자에게 속지 않는다. 첫 번째로, 다양한 피싱 주의 캠페인 등을 통해 사용자의 인식이 높아져 있고, 이제는 위와 같은 형태의 단순한 phishing site는 쉽게 인지한다. 또한, BoA(Bank of America)의 Site Key나 야후(Yahoo)의 Sign-in Seal 같은 피싱 방지 소프트웨어 등 단순한 피싱 방법에 효과적으로 대처하는 방법들이 등장하고 있다.

[0004] 이에 따라, 이제는 피싱 방법도 다음과 같은 형태로 진화하고 있다. 공식서버와 사용자 사이에서 MitM로(Man-in-the-Middle) 매우 정교하게 동작하며 사용자 모르게 트랜잭션(Transaction)을 변경하거나 사용자 정보를 탈취하는데, 이런 공격은 파밍(Pharming) 등과 결합되면서 더욱 인지하기 어려워지고 있다.

[0005] 따라서, 피싱 기술의 수준이 높아짐에 따라, 피싱 공격을 방어하기 위한 수단의 기술 수준이 향상되어야 할 필요성이 나타난다.

발명의 내용

해결하려는 과제

[0006] 본 발명의 실시예에 있어서, 사용자가 사이트에 접속하는 접속장치로 사용하는 PC의 지리적인 위치와 피싱 서버 등 중계 공격자(Man-in-the-middle Attacker)의 지리적 위치가 다르다는 점과, 대부분의 사용자는 휴대폰을 근접거리에 둔 채로 PC를 통해 서버에 접속한다는 점에 착안하여, 로그인 과정에 사용자 PC와 서버 사이에서 사용자 비밀 정보를 가져가거나 트랜잭션 요청을 변경하는 중계 공격자 형태의 피싱 공격을 방어할 수 있는 접속장치 인증 방법과 그 시스템을 제공하고자 한다.

과제의 해결 수단

[0007] 접속장치 인증 방법에 있어서, 서버에서 사용자의 휴대폰과 접속장치의 위치 정보를 수신하는 단계; 서버는 상기 접속장치로부터의 접속 시도를 식별하고, 휴대폰으로 접속장치의 위치 정보를 전송하는 단계; 및 서버는 미리 정해진 식별자를 이용한 상기 접속장치의 접속을 허용하는 단계를 포함하는 접속장치 인증 방법이 제공될 수 있다.

[0008] 일측에 있어서, 서버에서 사용자의 휴대폰과 접속장치의 위치 정보를 수신하는 단계에서 획득하는 위치 정보는 지피에스(GPS; Global Positioning System), 아이피 주소(IP Address; Internet Protocol Address), 맥 주소(MAC Address; Media Access Control Address) 중 적어도 하나를 이용하여 획득할 수 있다.

[0009] 또 다른 측면에 있어서, 접속장치의 위치 정보를 전송하는 단계는 푸시(Push) 알림, 문자 메시지, 음성 알림 중 적어도 하나의 방법으로 위치 정보를 휴대폰으로 전송할 수 있다.

[0010] 또 다른 측면에 있어서, 접속장치의 위치 정보를 전송하는 단계는 위치 정보를 전송하는 시기를 선택할 수 있다.

[0011] 또 다른 측면에 있어서, 서버에서 사용자의 휴대폰과 접속장치의 위치 정보를 수신하는 단계에서 획득하는 위치 정보는, 휴대폰과 접속장치의 거리 차이를 포함할 수 있다.

[0012] 또 다른 측면에 있어서, 접속장치의 위치 정보를 전송하는 단계는, 휴대폰과 접속장치의 거리 차이가 일정 거리 미만이라면, 위치 정보와 함께 서버로의 접속이 위험하지 않다는 신호를 휴대폰으로 전송하며, 휴대폰과 접속장치의 거리 차이가 일정 거리 이상이라면, 위치 정보와 함께 서버로의 접속이 위험하다는 경고 신호를 휴대폰으로 전송할 수 있다.

[0013] 또 다른 측면에 있어서, 접속장치의 접속을 허용하는 단계는 휴대폰과 접속장치의 거리 차이가 일정 거리 미만이라면, 접속장치의 접속을 허가하며, 휴대폰과 접속장치의 거리 차이가 일정 거리 이상이라면, 접속장치의 접속을 허가하지 않을 수 있다.

[0014] 또 다른 측면에 있어서, 접속장치의 접속을 허용하는 단계는 서버가 휴대폰으로부터 접속 허용 여부에 대한 메시지를 수신할 수 있다.

[0015] 또 다른 측면에 있어서, 접속장치의 접속을 허용하는 단계는 서버에서 제공하는 문자열 혹은 그림을 확인함으로써 비밀번호를 입력하도록 하여 접속장치의 접속을 허용하며, 문자열 혹은 그림은 서버에서 휴대폰으로 전송되거나 서버에 미리 등록될 수 있다.

[0016] 접속장치 인증 시스템에 있어서, 서버에서 사용자의 휴대폰과 접속장치의 위치 정보를 수신하는 위치 정보 수신부; 서버는 접속장치로부터의 접속 시도를 식별하고, 휴대폰으로 접속장치의 위치 정보를 전송하는 위치 정보 전송부; 및 서버는 미리 정해진 식별자를 이용한 접속장치의 접속을 허용하는 접속 제어부를 포함하는 접속장치 인증 시스템이 제공될 수 있다.

발명의 효과

[0017] 본 발명의 실시예에 따르면, 접속장치의 IP 주소, GPS 장치 등을 통해 위치 정보를 파악하여 사용자의 휴대폰으로 전송함으로써, 로그인 과정에 사용자 PC와 서버 사이에서 사용자 비밀 정보를 가져가거나 트랜잭션 요청을 변경하는 중계 공격자 형태의 피싱 공격을 방어할 수 있는 접속장치 인증 방법과 그 시스템을 제공할 수 있다.

도면의 간단한 설명

[0018] 도 1은 본 발명의 실시예에 있어서, 접속장치 인증 방법을 위한 시스템 환경을 도시한 것이다.

도 2는 본 발명의 실시예에 있어서, 접속장치 인증 방법의 단계를 도시한 흐름도이다.

도 3은 본 발명의 실시예에 있어서, 서버에 접속하기 위해 이루어지는 사용자 인증 방법을 도시한 흐름도이다.

도 4는 본 발명의 실시예에 있어서, 접속장치 인증 시스템의 구조를 도시한 블록도이다.

발명을 실시하기 위한 구체적인 내용

[0019] 이하, 접속장치 인증 방법 및 그 시스템에 대해서, 첨부된 도면을 참조하여 자세히 설명한다.

[0020] 본 발명의 실시예에 있어서, 피싱 공격을 방어하기 위해서, 사용자가 사이트에 접속하는 접속장치로 사용하는 PC의 지리적인 위치와 피싱 서버 등 중계 공격자(Man-in-the-middle Attacker)의 지리적 위치가 다르다는 점과, 대부분의 사용자는 휴대폰을 근접거리에 둔 채로 PC를 통해 서버에 접속한다는 점에 착안할 수 있다. 따라서, 로그인 과정에 사용자 PC와 서버 사이에서 사용자 비밀 정보를 가져가거나 트랜잭션 요청을 변경하는 중계 공격자 형태의 피싱 공격을 방어할 수 있는 접속장치 인증 방법과 그 시스템을 제공하고자 한다.

[0021] 본 발명의 실시예는 도 1과 같은 시스템 환경에서 실시될 수 있다. 실시예에 있어서, 사용자의 휴대폰(110)은 GPS(Global Positioning System)를 장착하고 있어 위치 정보를 서버(120)로 전송할 수 있으며, 스마트폰이나 피쳐폰 어느 하나에 제한되지 않는다.

[0022] 또한, 서버(120)는 고도의 보안을 필요로 하는 인증된 공식 사이트, 예컨대 은행이나 금융회사, 통신사 등의 공식 사이트, 또는 다양한 포털 사이트에 대한 접속을 관리할 수 있으며, 사용자의 휴대폰(110)과 접속장치(130)의 위치 정보를 저장하여 접속장치(130)로부터 특정 사이트 접속 시도가 감지되었을 때 저장된 위치 정보를 휴대폰(110)을 통해 사용자에게 전달할 수 있으며, 접속장치(130)의 서버(120) 접속에 대한 허가 여부를 결정할 수 있다.

[0023] 접속장치(130)는 GPS나 IP 주소(Internet Protocol Address), 혹은 맥 주소(MAC Address; Media Access Control Address) 등을 통해서 위치 정보를 서버(120)에 전송할 수 있으며, 접속장치(130)는 사이트에 접속할 수 있는 브라우저를 포함하는 장치로서 예컨대 PC나 노트북, 또는 스마트폰이나 태블릿 PC 등의 스마트 기기에 해당될 수 있다.

[0024] 본 발명의 실시예에 있어서, 발명에 사용될 수 있는 휴대폰(110)이나 접속장치(130)는 별도의 사용자 인증 혹은 등록을 필요로 할 수 있으며, 접속장치(130)와 휴대폰(110)의 사용자는 서로 일치할 수 있다.

[0025] 도 2는 본 발명의 실시예에 있어서, 휴대폰과 서버와 접속장치를 통해 실시되는 사이트에 접속하는 접속장치를 인증하는 방법의 단계를 간략히 도시한 흐름도이다. 실시예에 있어서, 서버는 휴대폰으로부터 휴대폰의 실시간 위치 정보를 수신할 수 있다(210). 또한, 마찬가지로 서버는 접속장치로부터 실시간 위치 정보를 수신할 수 있다(211). 단계(210)와 단계(211)의 동시에 실시될 수 있으며, 혹은 통신 환경에 따라서 어느 한 단계가 먼저 수행될 수 있다.

[0026] 실시간 위치 정보는 GPS나 IP 주소, 혹은 MAC 주소를 통해서 수집될 수 있으며, 서버로 전송되는 위치 정보는 약간의 오차를 동반할 수 있고, 일정한 시간 간격으로 수신하여 서버에 저장될 수 있다.

[0027] 서버는 접속장치가 사이트로 접속하고자 하는 시도를 식별할 수 있다(220). 여기서, 서버가 식별할 수 있는 사이트 접속은 서버에 인증을 완료한 공식 사이트에 대한 접속이다. 따라서, 피싱 사이트에 접속했다면 서버에서는 이를 식별할 수 없게 된다. 접속장치로부터의 사이트 접속 시도가 인지되면, 서버에서 수집한 접속장치와 휴대폰의 가장 최근의 위치 정보를 사용자의 휴대폰으로 전송할 수 있다(230). 위치 정보는 스마트폰에 대해서는 푸시(Push) 알림이 적용될 수 있으며, 다른 일례로는 문자 메시지, 음성 알림 등의 방법으로 위치 정보를 전송할 수 있다.

[0028] 실시예에 있어서, 접속장치 인증 방법은 접속장치로부터 접속 시도를 식별하는 단계(220)와 휴대폰과 접속장치의 위치 정보를 수신하는 단계(210, 211)는 순서가 바뀔 수 있는데, 일례를 들어 설명하면, 서버가 접속장치에서의 접속 시도를 식별하게 되면, 서버는 실시간으로 휴대폰과 접속장치의 위치 정보를 수신하여 사용자의 휴대폰으로 전송할 수 있다.

[0029] 실시예에 있어서, 단계(220)에서 위치 정보 알림 메시지를 전송하는 시기를 설정할 수 있는데, 예컨대 사용자의 서버 접속이 이루어진 이후에 전송할 수 있고, 사이트에 로그인이 완료된 시점에 혹은 사이트 내에서 거래가 이루어지기 전이나 후에 위치 정보 알림 메시지를 전송하도록 설정이 가능하다.

[0030] 본 발명의 실시예에 있어서, 서버는 휴대폰에 휴대폰과 접속장치의 위치 정보를 알린 이후에 휴대폰으로부터 접속장치의 접속 허가 여부를 수신함으로써 서버와 접속장치의 연결을 허가하거나 허가하지 않을 수 있다(231). 이때 서버는 휴대폰으로부터 수신한 접속 허가 여부를 따라 수행하며, 이에 따라 휴대폰과 접속장치에 안내 메시지를 전달할 수 있다.

[0031] 단계(231)는 휴대폰의 메시지를 수신하거나 휴대폰의 어플리케이션을 통해서, 또는 휴대폰의 웹 브라우저를 통해서 서버 접속의 허가 여부를 전달할 수 있으며, 혹은 사이트에 접속하려는 사용자 계정의 사용을 중지할 수 있는 기능을 포함함으로써 가능하다.

[0032] 또 다른 일례로, 서버는 휴대폰에 휴대폰과 접속장치의 위치 정보를 알린 이후에 어떤 사용자의 접속 시도인지를 확인하여 접속을 허가할 수 있다(240). 예컨대, 미리 서버에 접속장치의 위치 정보를 IP 주소나 MAC 주소를 통해 등록해 놓았거나, 별도의 식별자(예컨대, 쿠키 등)를 등록해 놓은 경우엔 휴대폰으로부터 별도의 접속 허가 여부를 수신하지 않고, 확인 후에 접속을 허가할 수 있다(240).

[0033] 상기와 같은 발명의 실시를 통해 서버에 접속할 때마다 접속장치와 휴대폰의 위치를 알리는 메시지를 사용자가 받을 수 있어, 만약 메시지가 수신되지 않는 다면 사용자가 접속한 사이트가 피싱 사이트임을 알아차릴 수 있으며, 또한 사용자가 서버에 접속하려는 시도가 없었는데 메시지가 수신되었다면 사용자의 계정이 해킹되고 있음을 의미할 수 있기에 해킹에 대비할 수 있게 된다.

[0034] 발명의 실시예에 있어서, 단계(210)와 단계(211)에서 수신한 사용자 휴대폰의 위치와 접속장치의 위치를 비교하여 접속장치의 위치에서 일정거리 이내에 사용자의 휴대폰이 있는지 없는지에 따라, 단계(230)에서 위치 정보를 전달할 때에 접속장치의 일정 반경거리 내에 휴대폰이 위치하고 있으면 접속이 위험하지 않다는 알림, 혹은 메시지를 함께 휴대폰으로 전달할 수 있으며, 반대로 일정 반경거리 내에 휴대폰이 위치하고 있지 않다면, 휴대폰으로 서버로의 접속이 위험할 수 있다는 경고 알림, 혹은 메시지를 함께 휴대폰으로 전달할 수 있다. 휴대폰으로 경고 메시지를 전달할 때엔 음성 또는 경고 알림음을 동반할 수 있다.

[0035] 또한, 서버에서는 단계(210)와 단계(211)에서 수신한 사용자 휴대폰과 접속장치의 위치의 거리 차이를 포함하여 저장할 수 있다. 따라서, 휴대폰과 접속장치의 거리 차이가 일정 거리 미만이라면, 단계(230)에서 위치 정보의 전송과 함께 서버로의 접속이 위험하지 않다는 신호 혹은 메시지를 휴대폰으로 전송할 수 있고, 휴대폰과 접속장치의 거리 차이가 일정 거리 이상이라면, 반대로 위치 정보의 전달과 함께 서버로의 접속이 위험하다는 경고 신호를 휴대폰으로 전송할 수 있다. 이러한 일례에도 휴대폰으로 경고 메시지를 전달할 때엔 음성 또는 경고 알림음을 동반할 수 있다.

[0036] 실시예에 있어서, 이와 같은 메시지를 휴대폰으로 전달한 이후에 서버는 휴대폰에 휴대폰과 접속장치의 위치 정보를 알린 이후에 휴대폰으로부터 접속장치의 접속 허가 여부를 수신함으로써 서버와 접속장치의 연결을 허가하거나 허가하지 않을 수 있다(231). 단계(231)는 휴대폰의 메시지를 수신하거나 휴대폰의 어플리케이션을 통해서, 또는 휴대폰의 웹 브라우저를 통해서 서버 접속의 허가 여부를 전달할 수 있으며, 혹은 사이트에 접속하려는 사용자 계정의 사용을 중지할 수 있는 기능을 포함함으로써 가능하다.

[0037] 또는, 서버는 휴대폰에 휴대폰과 접속장치의 위치 정보를 알린 이후에 어떤 사용자의 접속 시도인지를 확인하여 접속을 허가할 수 있다(240). 예컨대, 미리 서버에 접속장치의 위치 정보를 IP 주소나 MAC 주소를 통해 등록해 놓았거나, 별도의 식별자(예컨대, 쿠키 등)를 등록해 놓은 경우엔 휴대폰으로부터 별도의 접속 허가 여부를 수신하지 않고, 확인 후에 접속을 허가할 수 있다.

[0038] 예를 들어, 휴대폰에 '접속 지역과 휴대폰의 위치가 다릅니다. 현재 휴대폰을 소지하고 계시다면 접속한 사이트가 피싱 사이트일 수 있습니다. 접속 중이 아니시라면 누군가 xxx님의 아이디로 접속 시도 중입니다.' 라는 메시지가 수신된다면, 사용자는 다음과 같은 판단을 할 수 있다.

[0039] 현재 접속 시도 중이라면 휴대폰을 현재 소지하고 있지 않아서 위치가 다르게 식별된 것, 또는 현재 접속 중인 사이트가 피싱 사이트라는 것을 판단할 수 있으며, 접속 시도 중이 아닌 경우에 다음과 같은 메시지를 수신했다면 누군가 비밀번호를 해킹하고 있거나, 해킹되었다고 판단이 가능하다.

[0040] 본 발명의 실시예에 있어서, 서버에서는 단계(210)와 단계(211)에서 수신한 사용자 휴대폰과 접속장치의 위치 정보가 각 위치의 거리 차이를 포함할 수 있고, 접속장치로부터 접속 시도가 수신되었을 때(220), 서버는 휴대폰으로 위치 정보가 포함된 메시지를 송신할 수 있으며, 단계(231)를 생략하고 위치 정보에 포함되어 있는 휴대폰과 접속장치의 위치 거리 차이에 따라서 서버에서 접속을 허가하거나 허가하지 않을 수 있다.

[0041] 예컨대, 휴대폰에서 전송한 위치 정보, 휴대폰과 접속장치의 거리 차이가 일정 거리 미만일 때, 서버의 접속을 허가하고, 반대로 휴대폰과 접속장치의 거리 차이가 일정 거리 이상일 때, 서버는 사용자가 아닌 다른 이의 접속 시도로 간주하여 서버로의 접속을 허가하지 않는다.

[0042] 이와 같은 일례에는, 사용자가 휴대폰을 소지하고 있어야 접속장치를 통해 로그인이 가능하게 되기 때문에, 휴대폰을 소지하고 있지 않은 경우에 대해서는 단계(231)를 실시하여 접속 여부를 사용자의 휴대폰을 통해 수신할 수 있는 여지를 남겨둘 수 있다.

[0043] 피싱 사이트 중에 단순히 사용자의 아이디와 비밀번호 등을 탈취하려는 피싱 사이트의 경우, 본래 서버에 접속하지 않기 때문에 앞서 제시한 발명의 실시예가 동작하지 않는다. 따라서 도 3과 같은 서버 접속을 실시하도록 하여 피싱 서버가 원래의 서버에 접속해야 하는 상황을 만들어 발명의 실시예를 적용할 수 있다.

[0044] 도 3과 같이 서버에 접속하고(310), ID를 입력한(320) 이후에 바로 비밀번호를 입력하는 것이 아니라, 문자열이나 그림을 확인하여(330), 비밀번호를 입력할 수 있는(340) 절차를 가지는 로그인 방법에 사용자가 익숙해져 있어, 이와 다른 절차가 나타나면 인지할 수 있다는 가정하에 이하 발명의 실시예가 적용될 수 있다. 대부분의 사이트는 도 3의 단계(330)을 제외한 로그인 절차를 가진다.

[0045] 발명의 실시예에 있어서, 사용자가 서버에 접속하고(310), ID를 입력하는 단계(320)까지는 일치한다. 이후, 서버는 접속을 시도하는 접속장치를 등록된 IP 주소나 MAC 주소 등을 통해 식별한 후에, 사용자가 미리 등록해 놓은 문구 또는 이미지를 보여주고, 사용자가 등록한 문구 또는 그림과 일치하는지를 확인할 수 있다(330). 단계(330)는 단순히 보여주고 일치하는지의 여부를 확인하는 단계이다. 단계(330)에서 확인이 통과된 후에 서버는 비밀번호 입력창을 제공하여, 사용자는 비밀번호를 입력하여 로그인할 수 있다(340).

[0046] 또 다른 일례에 있어서, 사용자가 서버에 접속하고(310), ID를 입력하는 단계(320)가 실시된 이후, 서버가 휴대폰에 위치 정보를 포함하는 메시지를 전송하거나 알림할 때, 단계(330)에서 확인할 문자열이나 그림을 함께 포함하여 전송할 수 있다. 이에 따라, 서버는 접속장치의 로그인 페이지에 휴대폰으로 전송한 문자열이나 그림을 나타내고 사용자는 휴대폰에 수신된 문자열이나 그림과 일치하는지 확인할 수 있다(330). 마찬가지로, 단계(330)는 단순히 보여주고 일치하는지의 여부를 확인하는 단계가 될 수 있다. 이후, 서버는 비밀번호 입력창을 제공하여, 사용자는 비밀번호를 입력하여 로그인할 수 있다(340).

[0047] 만약, 피싱 서버가 원래 서버에 접속해서 해당 문자열이나 이미지를 가져가는 경우에 대해 설명하면, 피싱 서버는 사용자가 미리 등록했거나, 서버가 휴대폰으로 전송한 정상적인 문자열이나 이미지를 원래 서버에서 가져올 수는 있으나, 원래 서버에 접속하는 경우에 앞서 설명한 접속장치 인증 방법이 실시되기 때문에, 사용자에게 피싱 여부를 알리거나 접속을 제한할 수 있기 때문에 피싱 공격을 무력화시킬 수 있다.

[0048] 또한, 피싱 서버가 원래 서버에 접속하지 않는 경우엔, 앞선 일례의 접속장치 인증 방법은 실시되지 않지만, 사용자가 등록하거나 휴대폰에 수신된 문자열이나 이미지를 정상적으로 얻을 수 없기 때문에 로그인 과정에서 단계(330)를 표시할 수 없게 된다.

[0049] 따라서, 피싱 서버는 원래의 로그인 절차와 다른 절차, 즉 문자열이나 그림을 확인하는 단계(330)를 포함하지 않는 로그인 과정을 제공하게 되기 때문에, 도 3과 같은 로그인 과정에 익숙한 사용자로 하여금 현재 피싱 공격 상태임을 인지할 수 있게 하여, 이를 대비할 수 있다.

[0050] 본 발명의 실시예에 있어서, 도 4는 접속장치 인증 시스템(400)의 구조를 도시한 블록도이다. 접속장치 인증 시스템(400)은 도 1과 같은 환경에서 동작하는 시스템으로서, 접속장치 인증 방법을 실시할 수 있으며, 시스템(400)의 각 구조는 하나 이상으로 나누어질 수 있으며, 결합되어 동작할 수 있으며, 서버에 포함되어 동작할 수 있다.

[0051] 위치 정보 수신부(410)는 휴대폰으로부터 휴대폰의 실시간 위치 정보를 수신할 수 있다. 실시간 위치 정보는 GPS나 IP 주소, 혹은 MAC 주소를 통해서 수집될 수 있으며, 서버로 전송되는 위치 정보는 약간의 오차를 동반할 수 있다. 실시예에 있어서, 위치 정보는 일정한 시간 간격으로 수신하거나, 접속장치로부터 접속 시도가 식별되면 실시간으로 휴대폰과 접속장치의 위치 정보를 수신할 수 있다.

[0052] 또한, 위치 정보 전송부(420)는 접속장치로부터의 사이트 접속 시도가 인지되면, 서버에서 수집한 접속장치와 휴대폰의 가장 최근의 위치 정보를 사용자의 휴대폰으로 전송할 수 있다. 위치 정보는 스마트폰에 대해서는 푸시(Push) 알림이 적용될 수 있으며, 다른 일례로는 문자 메시지, 음성 알림 등의 방법으로 위치 정보를 전송할 수 있다.

[0053] 접속 제어부(430)는 휴대폰에 휴대폰과 접속장치의 위치 정보를 알린 이후에 어떤 사용자의 접속 시도인지를 확인하여 접속을 허가할 수 있다. 예컨대, 미리 서버에 접속장치의 위치 정보를 IP 주소나 MAC 주소를 통해 등록해 놓았거나, 별도의 식별자(예컨대, 쿠키 등)를 등록해 놓은 경우엔 휴대폰으로부터 별도의 접속 허가 여부를 수신하지 않고, 확인 후에 접속을 허가할 수 있다.

[0054] 또 다른 일례에 있어서, 접속 제어부(430)는 휴대폰에 휴대폰과 접속장치의 위치 정보의 알림과 함께 휴대폰으로부터 접속장치의 접속 허가 여부에 대한 알림을 함께 전송하고, 이에 대한 응답을 수신함으로써 서버와 접속장치의 연결을 허가하거나 허가하지 않을 수 있다.

[0055] 또한, 위치 정보 전송부(420)에서 전송한 위치 정보는 휴대폰과 접속장치의 거리 차이를 포함할 수 있는데, 휴대폰과 접속장치의 거리 차이가 일정 거리 미만일 때, 접속 제어부(430)는 서버의 접속을 허가하고, 반대로 휴대폰과 접속장치의 거리 차이가 일정 거리 이상일 때, 사용자가 아닌 다른 이의 접속 시도로 간주하여 서버로의 접속을 허가하지 않을 수 있다.

[0056] 실시예에 따른 피싱 공격을 방지하기 위한 접속장치 인증 방법은 다양한 컴퓨터 수단을 통하여 수행될 수 있는 프로그램 명령 형태로 구현되어 컴퓨터 판독 가능 매체에 기록될 수 있다. 상기 컴퓨터 판독 가능 매체는 프로그램 명령, 데이터 파일, 데이터 구조 등을 단독으로 또는 조합하여 포함할 수 있다. 상기 매체에 기록되는 프로그램 명령은 실시예를 위하여 특별히 설계되고 구성된 것들이거나 컴퓨터 소프트웨어 당업자에게 공지되어 사용 가능한 것일 수도 있다. 컴퓨터 판독 가능 기록 매체의 예에는 하드 디스크, 플로피 디스크 및 자기 테이프와 같은 자기 매체(Magnetic media), CD-ROM, DVD와 같은 광기록 매체(Optical media), 플롭티컬 디스크(Floptical disk)와 같은 자기-광 매체(Magneto-optical media), 및 롬(ROM), 램(RAM), 플래시 메모리 등과 같은 프로그램 명령을 저장하고 수행하도록 특별히 구성된 하드웨어 장치가 포함된다. 프로그램 명령의 예에는 컴파일러에 의해 만들어지는 것과 같은 기계어 코드뿐만 아니라 인터프리터 등을 사용해서 컴퓨터에 의해서 실행될 수 있는 고급 언어 코드를 포함한다. 상기된 하드웨어 장치는 실시예의 동작을 수행하기 위해 하나 이상의 소프트웨어 모듈로서 작동하도록 구성될 수 있으며, 그 역도 마찬가지이다.

[0057] 이상과 같이 실시예들이 비록 한정된 실시예와 도면에 의해 설명되었으나, 해당 기술분야에서 통상의 지식을 가진 자라면 상기의 기재로부터 다양한 수정 및 변형이 가능하다. 예를 들어, 설명된 기술들이 설명된 방법과 다른 순서로 수행되거나, 및/또는 설명된 시스템, 구조, 장치, 회로 등의 구성요소들이 설명된 방법과 다른 형태로 결합 또는 조합되거나, 다른 구성요소 또는 균등한 것들에 의하여 대치되거나 치환되더라도 적절한 결과가 달성될 수 있다.

[0058] 그러므로, 다른 구현들, 다른 실시예들 및 특허청구범위와 균등한 것들도 후술하는 특허청구범위의 범위에 속한다.

부호의 설명

[0059] 400: 접속장치 인증 시스템

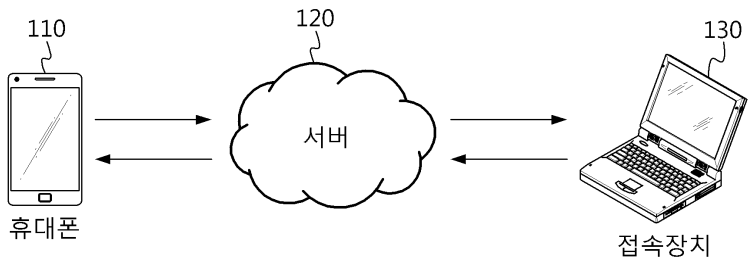
410: 위치 정보 수신부

420: 위치 정보 전송부

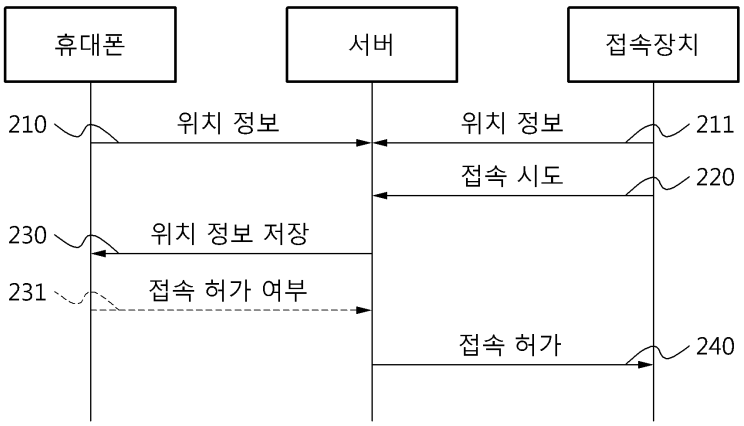
430: 접속 제어부

도면

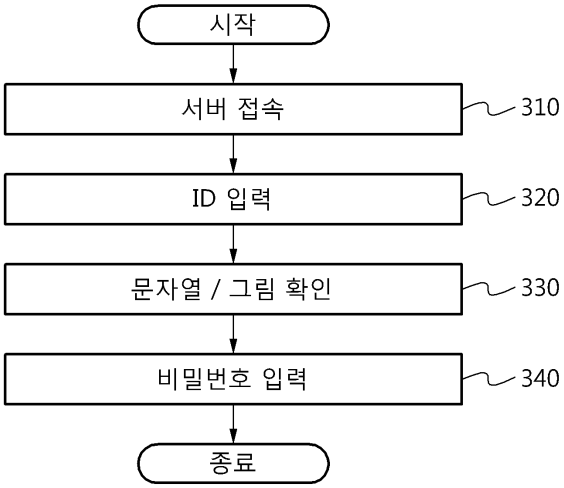
도면1



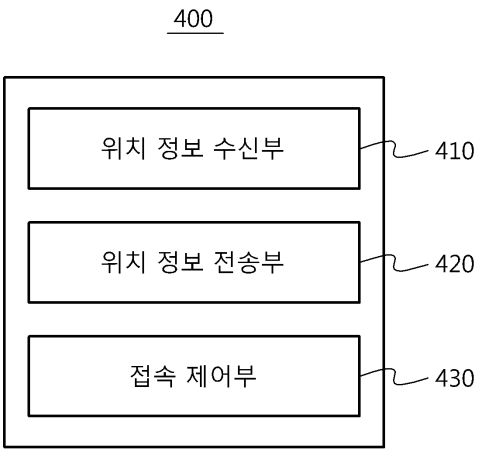
도면2


휴대폰
서버
접속장치
210
위치 정보
위치 정보
211
접속 시도
220
230
위치 정보 저장
231
접속 허가 여부
접속 허가
240

도면3


시작
서버 접속
310
ID 입력
320
문자열 / 그림 확인
330
비밀번호 입력
340
종료

도면4


400
위치 정보 수신부
410
위치 정보 전송부
420
접속 제어부
430