



República Federativa do Brasil
Ministério da Economia
Instituto Nacional da Propriedade Industrial

(21) BR 102020002913-4 A2



(22) Data do Depósito: 11/02/2020

(43) Data da Publicação Nacional: 06/10/2020

(54) Título: MÉTODO E SISTEMA PARA CONTROLAR A SEGURANÇA DE USUÁRIO DURANTE NAVEGAÇÃO NA INTERNET

(51) Int. Cl.: H04L 29/06.

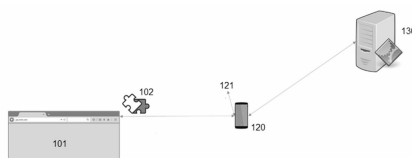
(52) CPC: H04L 63/18; H04L 63/0853.

(30) Prioridade Unionista: 12/02/2019 EP 19382098.2.

(71) Depositante(es): TELEFONICA DIGITAL ESPAÑA, S.L.U..

(72) Inventor(es): VICTOR MANUEL MUNDILLA GARCIA; ARUNA PREM BIANZINO; JOSE MARIA ALONSO CEBRIAN; SERGIO DE LOS SANTOS VILCHEZ.

(57) Resumo: MÉTODO E SISTEMA PARA CONTROLAR A SEGURANÇA DE USUÁRIO DURANTE NAVEGAÇÃO NA INTERNET. São fornecidos um método e um sistema para controlar a segurança de usuário durante navegação na internet. Um dispositivo de controle (120) recebe, por meio de um primeiro canal de comunicação, uma solicitação de página da Web de um agente de controle (102) implementado em um navegador (101), sendo que o navegador (101) é instalado em um dispositivo de computador operado por um usuário. Então, o dispositivo de controle (120) solicita, a um serviço de controle (130), por meio de um segundo canal de comunicação, um nível de segurança da dita página da Web solicitada, incluindo uma situação do usuário e a presença de riscos na página da Web solicitada. O serviço de controle (130) executa uma verificação de segurança na dita página da Web solicitada por meio de verificação da possibilidade da página da Web solicitada estar incluída em uma lista de bloqueios ou uma lista de permissões e também por meio de uma verificação de certos critérios de controle de risco da página da Web solicitada. Por fim, em resposta ao recebimento de um resultado da dita verificação de segurança, o dispositivo de controle (120) permite ou nega o acesso à dita página (...).



MÉTODO E SISTEMA PARA CONTROLAR A SEGURANÇA DE
USUÁRIO DURANTE NAVEGAÇÃO NA INTERNET

Campo Técnico

[001] Esta invenção se refere a um método, e sistema correspondente, para controlar a segurança de usuário durante navegação na Internet, em tempo real.

Antecedentes da Invenção

[002] Atualmente, a Internet oferece um acesso praticamente ilimitado a informações e entretenimento. Na maior parte do tempo, os usuários acessam tais informações e tal entretenimento através de navegadores, sendo expostos a uma grande variedade de riscos, de ataques de segurança, exposição de recursos e dados pessoais e corporativos confidenciais, até prisão ou coerção devido a algumas ações.

[003] Os usuários têm um grau muito baixo de consciência dos riscos que correm quando navegam na Internet. Ao mesmo tempo, todo tipo de regulamentação direcionada à conscientização do usuário é vista frequentemente pelo usuário como uma inconveniência, e usuários tendem a aceitar sempre qualquer tipo de notificação/aviso sem lê-lo, ao ponto de softwares específicos terem sido projetados para evitar automaticamente mensagens de alerta. Por fim, usuários tendem a fazer o que são instruídos a fazer, mesmo se não estiverem cientes dos resultados, sendo expostos, desse modo, a outros riscos.

[004] Nesse contexto, diferentes soluções estão disponíveis para controlar o acesso à internet de um usuário, em geral tendo como objetivo o Controle Parental. As soluções disponíveis definem geralmente critérios estáticos para diferenciar o conteúdo e as operações disponíveis para um

usuário (eventualmente com base em bancos de dados externos) e geralmente oferecem uma decisão estática sobre a solicitação. Nos casos em que um usuário de controle está envolvido, é solicitada a ele uma decisão sem informação/suporte.

[005] Algumas patentes e pedidos de patente são conhecidos no campo.

[006] O documento US 2013017806 A1 revela um sistema para controlar o acesso à internet de um dispositivo móvel (controle parental), permitindo que outro dispositivo móvel (o controlador) defina critérios para a navegação do usuário, incluindo localização e momento do dia/semana. Ao contrário da presente invenção, essa solução tem como objetivo apenas dispositivos móveis como dispositivos controlados. Essa solução tem como objetivo apenas o controle parental e não a segurança de um usuário genérico durante a navegação na internet. Essa solução não é interativa e não permite um controle em tempo real sobre os dispositivos controlados e sua atividade.

[007] O documento US 8571538 B2 fornece um sistema para gerar dinamicamente controle parental baseado em comunidade para dispositivos celulares baseados na maioria das definições de controle parental mais comuns selecionadas por membros da comunidade. Os critérios para controlar o acesso do dispositivo controlado podem ser baseados em diferentes perfis, os quais são desenvolvidos com base nos perfis comuns de controle parental presentes na comunidade. O controlador (os pais) pode selecionar um dos conjuntos de critérios da "comunidade" disponíveis e editá-lo. Os conjuntos de critérios da comunidade são constantemente atualizados com base nas escolhas da parte de controladores da comunidade. Essa solução

tem como objetivo apenas dispositivos móveis como dispositivos controlados. Essa solução tem como objetivo apenas o controle parental e não a segurança de um usuário genérico durante a navegação na internet. Essa solução não é interativa e não permite um controle em tempo real sobre os dispositivos controlados e sua atividade, mesmo se permitir alterações na definição de critérios pelo controlador.

[008] O documento US 2015365379 A1 fornece um sistema para aprender de forma inteligente uma lista de conteúdos de IP permitidos em um ou mais dispositivos conectados à internet implementando um meio de controle parental inteligente. O meio inclui um roteador e um filtro. O filtro é implementado no roteador que conecta o dispositivo à internet. Com base em um período de aprendizado, o sistema aprende quais são os conteúdos com permissão para navegação. Isso gera uma lista de permissões, a qual pode ser modificada posteriormente pelo controlador através de outro dispositivo conectado ao roteador. Ao contrário da presente invenção, essa solução tem como objetivo apenas o controle parental e não a segurança de um usuário genérico durante a navegação na internet. Essa solução não é interativa e não permite um controle em tempo real sobre os dispositivos controlados e sua atividade, mesmo se o controlador receber alertas em tempo real se o dispositivo controlado estiver tentando acessar um conteúdo negado pela política. Ainda assim, o alerta é baseado na política e não dinamicamente no conteúdo, permitindo apenas o controle de conteúdo e riscos conhecidos.

[009] O documento US 20150347769 A1 define uma hierarquia entre usuários. Os usuários em um nível hierárquico inferior devem solicitar permissão para os usuários em um nível

hierárquico superior para acessar o conteúdo da internet "restrito" (ou para realizar outras operações restritas). O controlador pode ignorar a solicitação ou conceder a permissão. Essa solução contempla apenas o caso em que os diferentes dispositivos envolvidos são usados por diferentes usuários finais. As restrições para realizar operações para o usuário controlado são definidas com base no tipo de operação (por exemplo, comprar, acessar um tipo específico de conteúdo, etc.), em uma base estática, e não são analisadas em tempo real.

[010] Técnicas/soluções inovadoras são, portanto, necessárias para controle de segurança em tempo real da navegação que funciona tanto para o controle de segurança sobre outro usuário quanto para autocontrole de segurança.

Descrição da Invenção

[011] Com essa finalidade, modalidades da presente invenção fornecem, de acordo com um primeiro aspecto, um método para controlar navegação na internet. O método compreende receber, por um dispositivo de controle, como um telefone móvel, por meio de um primeiro canal de comunicação, uma solicitação de página da Web proveniente de um agente de controle implementado em um navegador. O navegador é instalado em um dispositivo de computador, como um PC, um laptop ou um tablet, entre outros, operado por um usuário. A solicitação da Web inclui um endereço da Web solicitado pelo usuário e informações de identificação de usuário. O dispositivo de controle solicita então a um serviço de controle, por meio de um segundo canal de comunicação, um nível de segurança da dita página da Web solicitada, incluindo uma situação do usuário e a presença de riscos na página da Web solicitada. O serviço de

controle executa uma verificação de segurança na dita página da Web solicitada por meio de verificação da possibilidade da página da Web solicitada estar incluída em uma lista de bloqueios ou uma lista de permissões e também por meio de uma verificação de certos critérios de controle de risco da página da Web solicitada. Por fim, em resposta ao recebimento de um resultado da dita verificação de segurança do serviço de controle, o dispositivo de controle compreende permitir ou negar o acesso à dita página da Web.

[012] Em uma modalidade particular, o primeiro canal de comunicação é diferente do segundo canal de comunicação. Por exemplo, o primeiro canal de comunicação inclui uma comunicação por Bluetooth e a segunda comunicação inclui uma tecnologia de internet sem fio como 3G, 4G ou 5G.

[013] Em uma modalidade, os ditos critérios de controle de risco compreendem pelo menos uma opção dentre as seguintes: verificar se o conteúdo da página da Web solicitada é compatível com uma lista de bloqueios específica; verificar se o endereço da Web inclui erros de digitação; verificar se o conteúdo da página da Web solicitada inclui operações de risco, como solicitação de dados pessoais, senha, etc.; verificar se o conteúdo da página da Web solicitada inclui conteúdo indesejado, incluindo conteúdo violento e/ou pornográfico; verificar se o conteúdo da página da Web solicitada inclui código malicioso e/ou verificar a autenticidade de um certificado do endereço da Web.

[014] Em uma modalidade, o resultado da verificação de segurança é transmitido pelo serviço de controle para o dispositivo de controle na forma de uma mensagem. Caso o resultado da verificação de segurança indique que um risco

potencial foi detectado, um nível e tipo de risco podem ser adicionalmente especificados na mensagem.

[015] De acordo com o método proposto, dependendo de uma configuração de usuário e do nível e tipo de risco detectado, o dispositivo de controle pode negar o acesso à página da Web, permitir o acesso à mesma ou solicitar uma aprovação manual de um usuário de controle, sendo que esse último supervisiona o dispositivo de controle. Caso uma aprovação manual seja necessária, o usuário de controle pode solicitar adicionalmente uma decisão de suporte para o serviço de controle. A decisão de suporte é tomada mediante o recebimento pelo usuário de controle de um ou mais dos seguintes dados: tipo de risco, incluindo conteúdo da lista de bloqueios, erro de digitação no endereço da Web, operação de risco, conteúdo indesejado, código malicioso, etc.; dados específicos relacionados ao risco, incluindo tipo de operação de risco, dados confidenciais que a página da Web solicitou, um domínio, etc. e/ou uma captura de tela da página da Web solicitada.

[016] Em uma modalidade, o dispositivo de controle envia adicionalmente uma notificação ao usuário de controle indicando se o acesso do usuário à página da Web solicitada foi negado ou permitido.

[017] Ainda em outra modalidade, se o acesso à página da Web for negado, o serviço de controle armazena a página da Web solicitada em um arquivo do mesmo.

[018] Modalidades da presente invenção também fornecem, de acordo com um segundo aspecto, um sistema para controlar a navegação na internet. O sistema inclui:

[019] - um navegador instalado em um dispositivo

de computação (por exemplo, um computador) operado por um usuário;

[020] - um agente de controle (por exemplo, uma extensão do navegador) implementado no dito navegador;

[021] - um dispositivo de controle (por exemplo, um telefone móvel); e

[022] - um serviço de controle (por exemplo, um servidor remoto, como um servidor de computador em nuvem, entre outros).

[023] O dispositivo de controle tem uma primeira unidade de comunicação para receber, do agente de controle, uma solicitação de página da Web, incluindo um endereço da Web solicitado pelo usuário e informações de identificação de usuário, e uma segunda unidade de comunicação para solicitar, para o serviço de controle, um nível de segurança da dita página da Web solicitada, incluindo uma situação do usuário e a presença de riscos na página da Web solicitada, e para receber uma resposta de uma verificação de segurança executada pelo serviço de controle.

[024] O dispositivo de controle é configurado para permitir ou negar acesso à página da Web, considerando a dita resposta recebida.

[025] De acordo com o sistema proposto, a primeira e a segunda unidades de comunicação do dispositivo de controle podem ser iguais ou diferentes. Caso sejam diferentes, a primeira unidade de comunicação compreende uma unidade de comunicação por Bluetooth e a segunda unidade de comunicação compreende uma unidade de comunicação sem fio, incluindo WiFi.

[026] A presente invenção garante então uma análise em tempo real das operações tentadas pelo usuário

controlado; distância máxima entre o controlador e os dispositivos controlados conectados por tecnologia (problemas de segurança reduzidos e negação, desde a concepção, do uso do dispositivo controlado quando o usuário de controle está distante); resiliência, desde a concepção, a ataques do tipo Man-in-the-Middle devido ao uso de canais laterais; resiliência, desde a concepção, a ataques e infecção do dispositivo controlado, já que o controle é executado em um dispositivo diferente e com o uso de um canal de rede diferente; controle de risco é realizado em um dispositivo diferente (definitivamente não afetado por malware).

Breve Descrição dos Desenhos

[027] As vantagens e características anteriores e outras serão mais completamente compreendidas a partir da seguinte descrição detalhada das modalidades, em referência às figuras anexas, que devem ser consideradas de uma maneira ilustrativa e não limitativa, em que:

A Fig. 1 mostra graficamente a arquitetura de sistema da presente invenção de acordo com uma modalidade.

A Fig. 2 é um diagrama que mostra que o usuário tenta abrir uma página da Web, cujo conteúdo é detectado como sem risco pelo serviço de controle.

A Fig. 3 é um diagrama que mostra que o usuário tenta abrir uma página da Web, cujo conteúdo é detectado como de risco pelo serviço de controle. O usuário de controle, após avisado, permite que o usuário navegue o conteúdo solicitado.

A Fig. 4 é um diagrama que mostra que o usuário tenta abrir uma página da Web, cujo conteúdo é detectado como de risco pelo serviço de controle. O usuário de controle, após avisado, impede que o usuário navegue o conteúdo solicitado.

A Fig. 5 é um diagrama que mostra que o usuário tenta abrir uma página da Web, cujo conteúdo é detectado como da lista de bloqueios pelo serviço de controle.

Descrição Detalhada de Modalidade Preferenciais

[028] A Fig. 1 ilustra uma modalidade da arquitetura do sistema proposto. De acordo com essa modalidade, um usuário (não ilustrado na figura) está acessando a Internet 140 através de um navegador 101, a partir de um dispositivo de computador genérico (por exemplo, um dispositivo de computador móvel ou fixo) e em particular através de um navegador 101 instalado no dito dispositivo de computador, operado pelo usuário. O navegador 101 inclui um agente de controle 102, por exemplo, implementado como uma extensão do navegador, que se comunica com um dispositivo de controle 120, como um dispositivo de telefone, entre outros. O dispositivo de controle 120 é gerenciado por um usuário de controle 121 e pode se comunicar com um serviço de controle 130. O serviço de controle 130 pode estar localizado na Internet 140 e pode ser implementado como um serviço externo ao usuário.

[029] O dispositivo de controle 120 pode incluir um aplicativo de software específico (por exemplo, um app) para gerenciar a comunicação com o agente de controle 102, o usuário de controle 121 e o serviço de controle 130 e para avaliar as solicitações de navegação. Particularmente, o dispositivo de controle 120 faz interface com o serviço de controle 130 através de APIs específicas.

[030] Em uma modalidade particular, a comunicação entre o agente de controle 102 e o dispositivo de controle 120 é realizado através de um primeiro canal de comunicação, por exemplo, por meio de Bluetooth, enquanto a

comunicação entre o dispositivo de controle 120 e o serviço de controle 130 ocorre através de um segundo canal de comunicação, diferente do primeiro canal de comunicação, a fim de impedir ataques de segurança como Man-in-the-Middle (MitM). Uma escolha possível para o segundo canal de comunicação pode ser implementada com o uso de conectividade 3G/4G/5G. Do mesmo modo, um alcance limitado de conectividade entre o dispositivo de computador (a saber, o dispositivo de computador controlado, isto é, o dispositivo de computador que tem o navegador 101 instalado no mesmo) e o dispositivo de controle 120 permite que se impeça o uso do dispositivo de computador quando o usuário de controle 121 está distante. O uso de um dispositivo diferente como o dispositivo de controle 120 também permite que se impeça um possível malware presente no dispositivo de computador controlado.

[031] Entretanto, o uso de dois canais de comunicação diferentes não é obrigatório na presente invenção.

[032] De acordo com a invenção proposta, quando uma página da Web é solicitada pelo usuário, o agente de controle 102 encaminha o endereço da Web (isto é, o URL) juntamente a outras informações de identificação necessárias do usuário (por exemplo, um identificador) para o dispositivo de controle 120, o qual responderá permitindo ou negando a operação. Em particular, após o dispositivo de controle 120 receber o endereço da Web e as informações de identificação de usuário sobre uma solicitação de página da Web do agente de controle 102, ele consultará o serviço de controle 130 sobre o nível de segurança do conteúdo solicitado, mantendo a definição do usuário solicitante, e a presença de riscos eventuais no mesmo.

[033] O serviço de controle 130 está na primeira definição para o usuário de controle 121 especificando eventuais listas de bloqueio e/ou listas de permissão, bem como critérios de controle de risco (tipo de riscos notificado, nível de notificação de risco, etc.). De modo alternativo ou complementar, uma definição diferente pode ser especificada para cada par de usuário de controle-usuário controlado e é armazenada em um arquivo de configuração no serviço de controle 130.

[034] Os critérios de controle de risco que podem ser verificados pelo serviço de controle 130 podem incluir, porém sem limitação:

- Conteúdo compatível com uma lista de bloqueios específica. A lista de bloqueio pode ser definida pelo usuário de controle 121 e/ou pode ser baseada em listas de bloqueio compartilhadas disponíveis em repositórios específicos, incluindo URLs maliciosos conhecidos, etc.
- Endereço da Web, incluindo erros de digitação. Uma possível implementação desse controle pode incluir, por exemplo, a verificação contra um dicionário/repositório.
- Conteúdo incluindo operações de risco, por exemplo, solicitação de dados confidenciais (número de conta, dados pessoais, etc.), solicitação de nome de usuário/senha, etc.
- Conteúdo incluindo conteúdo indesejado, por exemplo, violência, pornografia, etc.
- Presença de código malicioso, por exemplo, execução de scripts externos, redirecionamentos coercivos, falsificação de DNS, etc.
- Não autenticidade do certificado associado ao

endereço da Web.

[035] Após o serviço de controle 130 responder sobre uma solicitação de página da Web, o dispositivo de controle 120, finalmente envolvendo e informando o usuário de controle 121, impõe a política adequada à solicitação de página da Web.

[036] Com base nos riscos identificados e na definição de nível de segurança para o usuário, os seguintes resultados são possíveis:

- Se o serviço de controle 130 não detectar riscos potenciais com base nas verificações acima, uma mensagem de OK é devolvida ao dispositivo de controle 120, o qual, desse modo, prossegue para o encaminhamento da solicitação de página da Web original para a Internet 140, a qual responderá como de costume ao usuário controlado. Consultar Fig. 2 para um exemplo desse tipo de transação.

- Se o serviço de controle 130 detectar qualquer risco potencial com base nas verificações acima, uma notificação é enviada para o dispositivo de controle 120. Um nível e um tipo de risco são especificados na mensagem de notificação. Dependendo da definição para o usuário específico e do tipo e nível de risco identificado, o dispositivo de controle 120 bloqueia a solicitação de página da Web, permite-a ou solicita a aprovação manual do usuário de controle 121 para prosseguir com o conteúdo solicitado. No caso de aprovação manual, o usuário de controle 121 é informado para que apoie sua decisão, como especificado abaixo.

[037] O aplicativo de software específico implementa as funcionalidades de controle e a interface com o agente de controle 102, o usuário de controle 121 e o serviço

de controle 130. O aplicativo de software informa o usuário de controle 121 de uma tentativa de acesso a um conteúdo potencialmente de risco proveniente do navegador controlado 101 e o apoia na tomada de uma decisão informada sobre permitir ou não o acesso à página da Web solicitada. As informações para apoiar o usuário de controle 121 podem incluir o tipo de risco (conteúdo da lista de bloqueios, erro de digitação no endereço da Web, operação de risco, conteúdo indesejado, código malicioso, etc.), informações específicas relacionadas ao risco (por exemplo, se a solicitação incluir uma operação de risco, o usuário de controle 121 é informado sobre o tipo de operação, os dados confidenciais que a operação solicita, o domínio que solicita tais informações, etc.), uma captura de tela/pré-visualização da página da Web solicitada (ainda não mostrada para o usuário controlado), possivelmente posicionada lado a lado com o conteúdo verdadeiro correspondente suposto (por exemplo, no caso de detecção de sequestro de URL (typosquatting), uma pré-visualização é mostrada da página solicitada lado a lado a uma pré-visualização da página sequestrada), um resultado de solicitações anteriores contra solicitações de conteúdo iguais ou similares, e possíveis informações adicionais que podem ser relevantes para que o usuário de controle 121 tome uma decisão informada. Essas informações de suporte são fornecidas pelo serviço de controle 130.

[038] O usuário de controle 121 toma, desse modo, uma decisão informada sobre negar/permitir que o usuário controlado acesse a página da Web solicitada. No caso de negação, consultar a Fig. 4, o agente de controle 102 bloqueia a solicitação (isto é, não a encaminha para a Internet 140) e

notifica o usuário controlado sobre o acesso negado ao conteúdo solicitado. A ação selecionada pelo usuário de controle 121 é registrada no arquivo de configuração do serviço de controle 130, associado à página da Web solicitada, para apoiar futuras escolhas sobre solicitações similares ou iguais.

[039] No caso de permissão, consultar a Fig. 3, o agente de controle 102 encaminha a solicitação de página da Web para a Internet 140 como era originalmente, para que a resposta da Web alcance diretamente o usuário controlado de modo que seja transparente tanto para o usuário controlado quanto para o servidor de internet que recebe a solicitação. A ação selecionada pelo usuário de controle 121 é registrada no arquivo de configuração do serviço de controle 130, associado à página da Web solicitada, para apoiar futuras escolhas sobre solicitações similares ou iguais.

[040] Por fim, o serviço de controle 130 pode identificar a página da Web solicitada como expressamente proibida, dependendo da definição especificada (por exemplo, tipo de risco, tipo de conteúdo, endereço da Web específico, etc.). Nesse caso, nenhuma aprovação manual é solicitada ao usuário de controle 121 e a solicitação de navegação do usuário controlado é diretamente negada. Dependendo da definição do usuário, o usuário de controle 121 pode ser notificado da solicitação pelo usuário controlado por meio do dispositivo de controle 120. Consultar Fig. 5 para um exemplo desse tipo de transação.

[041] O usuário pode ser o mesmo usuário que controla o dispositivo de controle 120 (por exemplo, no caso de autoproteção de riscos de navegação), ou um usuário diferente (por exemplo, no caso de controle parental ou

controle hierárquico).

[042] Ademais, o dispositivo de controle 120 pode controlar múltiplos navegadores 101, usados por diferentes usuários ou pelo mesmo usuário. Nesse caso, a notificação de risco enviada para o dispositivo de controle 120 também incluirá um identificador do usuário correspondente/navegador/dispositivo de computador controlado.

[043] Diferentes usuários de controle 121 podem ser habilitados no mesmo sistema e podem controlar juntamente os mesmos usuários (ou conjunto de usuários). Nesse caso, uma autorização múltipla ou única pode ser configurada para o sistema. No primeiro caso, todos os usuários de controle 121 devem autorizar a solicitação de página da Web de risco antes que seja aceita, enquanto no último caso um único usuário de controle 121 é notificado, e sua resposta é usada para selecionar se a solicitação de página da Web é encaminhada ou negada. O usuário de controle específico 121 a ser notificado pode ser selecionado com base em uma hierarquia definida, com base no carimbo de data e horário de registro dos diferentes usuários de controle 121 no sistema, ou com base em uma política de distribuição de carga (por exemplo, Round Robin, entre outros). O usuário de controle 121 permite redundantemente que o sistema trabalhe como esperado (isto é, aceitação/rejeição pelo usuário de controle 121) também quando um usuário de controle 121 sai da área do sistema. Por outro lado, uma política padrão pode ser definida para os casos em que nenhum usuário de controle 121 está disponível na área de sistema (isto é, rejeitar ou permitir). Em qualquer caso, a configuração selecionada deveria ser configurada no sistema

durante sua definição.

[044] As modalidades descritas acima devem ser compreendidas como alguns exemplos ilustrativos da presente invenção. Será compreendido por aqueles que são versados na técnica que várias modificações, combinações e alterações podem ser feitas nas modalidades sem que haja desvio do escopo da presente invenção. Em particular, soluções de diferentes partes nas diferentes modalidades podem ser combinadas em outras configurações, quando tecnicamente possível.

[045] O escopo da presente invenção é definido no seguinte conjunto de reivindicações.

REIVINDICAÇÕES

1. MÉTODO PARA CONTROLAR A SEGURANÇA DE USUÁRIO DURANTE NAVEGAÇÃO NA INTERNET, sendo o método caracterizado por compreender:

- receber, por um dispositivo de controle (120), por meio de um primeiro canal de comunicação, uma solicitação de página da Web de um agente de controle (102) implementado em um navegador (101), em que o navegador (101) é instalado em um dispositivo de computador operado por um usuário e a solicitação da Web, incluindo um endereço da Web solicitado pelo usuário e informações de identificação de usuário;

- solicitar, pelo dito dispositivo de controle (120), a um serviço de controle (130), por meio de um segundo canal de comunicação, um nível de segurança da dita página da Web solicitada, incluindo uma situação do usuário e a presença de riscos na página da Web solicitada;

- executar, pelo serviço de controle (130), uma verificação de segurança na dita página da Web solicitada por meio de verificação da possibilidade da página da Web solicitada estar incluída em uma lista de bloqueios ou uma lista de permissões e também por meio de uma verificação de certos critérios de controle de risco da página da Web solicitada; e

- em resposta ao recebimento de um resultado da dita verificação de segurança do serviço de controle (130), o dispositivo de controle (120) permite ou nega acesso à dita página da Web.

2. MÉTODO, de acordo com a reivindicação 1, caracterizado pelo primeiro canal de comunicação ser diferente do segundo canal de comunicação.

3. MÉTODO, de acordo com a reivindicação 2, caracterizado pelo primeiro canal de comunicação incluir uma comunicação por Bluetooth e a segunda comunicação incluir uma tecnologia de internet sem fio, incluindo 3G, 4G ou 5G.

4. MÉTODO, de acordo com a reivindicação 1, caracterizado pelos ditos critérios de controle de risco compreenderem pelo menos um dos seguintes:

- verificar se o conteúdo da página da Web solicitada é compatível com uma lista de bloqueios específica;
- verificar se o endereço da Web inclui erros de digitação;
- verificar se o conteúdo da página da Web solicitada inclui operações de risco;
- verificar se o conteúdo da página da Web solicitada inclui conteúdo indesejado, incluindo conteúdo violento e/ou pornográfico;
- verificar se o conteúdo da página da Web solicitada inclui código malicioso; e/ou
- verificar a autenticidade de um certificado da endereço da Web.

5. MÉTODO, de acordo qualquer uma das reivindicações 1 a 4, caracterizado pelo dito resultado da verificação de segurança sendo transmitido pelo serviço de controle (130) para o dispositivo de controle (120) na forma de uma mensagem, em que, se o resultado da verificação de segurança indicar que um risco potencial foi detectado, um nível e um tipo de risco serem especificados na mensagem.

6. MÉTODO, de acordo com a reivindicação 5, caracterizado por, dependendo de uma configuração de usuário

e do nível e tipo de risco, o dispositivo de controle (120) nega o acesso à página da Web, permitir o acesso à mesma ou solicita uma aprovação manual de um usuário de controle (121), sendo que o último supervisiona o dispositivo de controle (120).

7. MÉTODO, de acordo com a reivindicação 6, caracterizado por, se uma aprovação manual for solicitada, o usuário de controle (121) solicitar adicionalmente uma decisão de suporte ao serviço de controle (130), em que a dita decisão de suporte é tomada mediante o recebimento de um ou mais dos dados a seguir:

- tipo de risco, incluindo conteúdo da lista de bloqueios, erro de digitação no endereço da Web, operação de risco, conteúdo indesejado, código malicioso;

- dados específicos relacionados ao risco, incluindo tipo de operação de risco, dados confidenciais que a página da Web solicitou, um domínio; e/ou

- uma captura de tela da página da Web solicitada, preferencialmente posicionada lado a lado à página da Web verdadeira correspondente suposta.

8. MÉTODO, de acordo com a reivindicação 1, caracterizado por compreender adicionalmente enviar, pelo dispositivo de controle (120), uma notificação para um usuário de controle (121) sobre negar/permitir que o usuário acesse a página da Web solicitada.

9. MÉTODO, de acordo com a reivindicação 1, caracterizado por, se o acesso à dita página da Web for negado, o serviço de controle (130) armazenar adicionalmente a página da Web solicitada em um arquivo do mesmo.

10. SISTEMA PARA CONTROLAR A SEGURANÇA DE USUÁRIO

DURANTE NAVEGAÇÃO NA INTERNET, caracterizado por compreender:

- um navegador (101) instalado em um dispositivo de computação operado por um usuário;
- um agente de controle (102) implementado no dito navegador (101);
- um dispositivo de controle (120); e
- um serviço de controle (130);

em que o dispositivo de controle tem uma primeira unidade de comunicação para receber, do agente de controle (102), uma solicitação de página da Web, incluindo um endereço da Web solicitado pelo usuário e informações de identificação de usuário; e uma segunda unidade de comunicação para solicitar, ao serviço de controle (130), um nível de segurança da dita página da Web solicitada, incluindo uma situação do usuário e a presença de riscos na página da Web solicitada, e para receber uma resposta de uma verificação de segurança executada pelo serviço de controle (130), e

em que o dispositivo de controle (120) é configurado para permitir ou negar o acesso à dita página da Web solicitada considerando a dita resposta recebida.

11. SISTEMA, de acordo com a reivindicação 10, caracterizado pela primeira unidade de comunicação ser diferente da segunda unidade de comunicação.

12. SISTEMA, de acordo com qualquer uma das reivindicações 10 ou 11, caracterizado pela primeira unidade de comunicação compreender uma unidade de comunicação por Bluetooth e a segunda unidade de comunicação compreende uma unidade de comunicação sem fio, incluindo 3G, 4G ou 5G.

13. SISTEMA, de acordo com a reivindicação 10,

caracterizado pelo o dispositivo de controle (120) ser um telefone móvel.

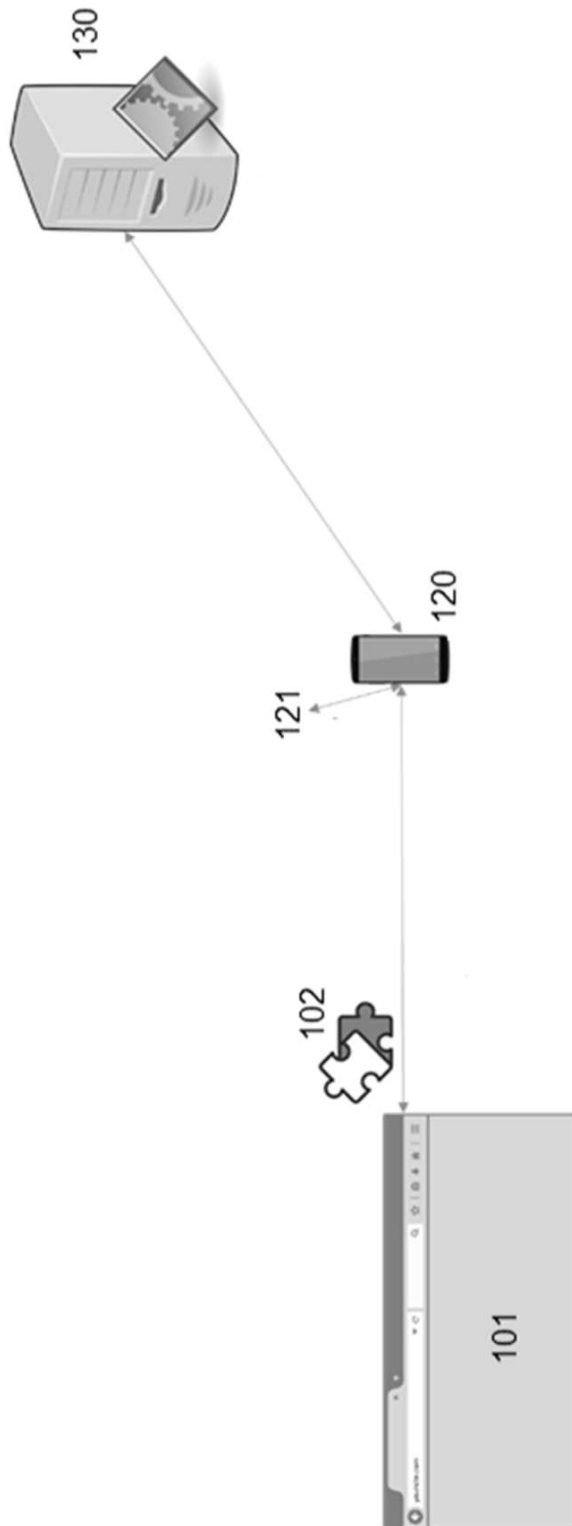


Fig. 1

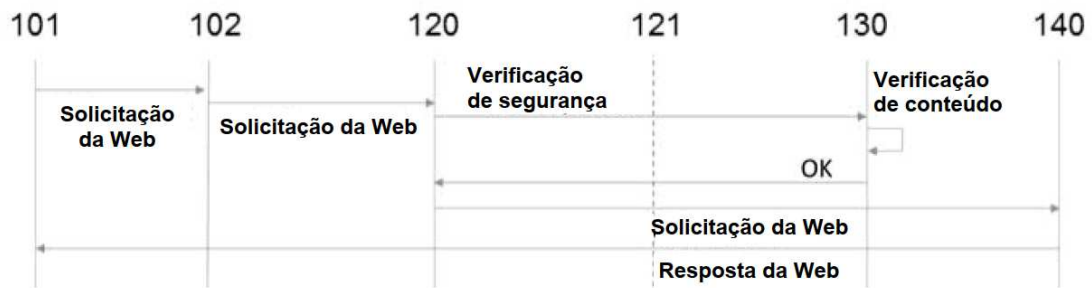


Fig. 2



Fig. 3

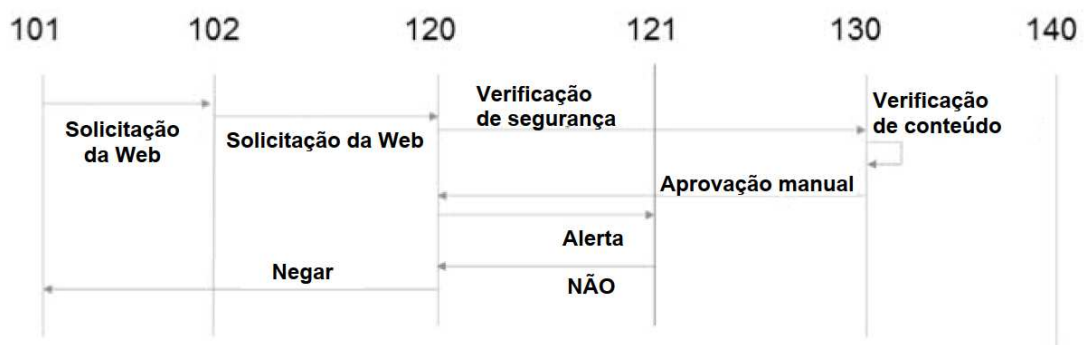


Fig. 4

**Fig. 5**

RESUMOMÉTODO E SISTEMA PARA CONTROLAR A SEGURANÇA DE
USUÁRIO DURANTE NAVEGAÇÃO NA INTERNET

São fornecidos um método e um sistema para controlar a segurança de usuário durante navegação na internet. Um dispositivo de controle (120) recebe, por meio de um primeiro canal de comunicação, uma solicitação de página da Web de um agente de controle (102) implementado em um navegador (101), sendo que o navegador (101) é instalado em um dispositivo de computador operado por um usuário. Então, o dispositivo de controle (120) solicita, a um serviço de controle (130), por meio de um segundo canal de comunicação, um nível de segurança da dita página da Web solicitada, incluindo uma situação do usuário e a presença de riscos na página da Web solicitada. O serviço de controle (130) executa uma verificação de segurança na dita página da Web solicitada por meio de verificação da possibilidade da página da Web solicitada estar incluída em uma lista de bloqueios ou uma lista de permissões e também por meio de uma verificação de certos critérios de controle de risco da página da Web solicitada. Por fim, em resposta ao recebimento de um resultado da dita verificação de segurança, o dispositivo de controle (120) permite ou nega o acesso à dita página da Web.