



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

(11) BR 112014006261-7 B1



(22) Data do Depósito: 14/09/2012

(45) Data de Concessão: 13/07/2021

(54) Título: MÉTODO PARA IMPEDIR A MANIPULAÇÃO DE PÁGINA DA WEB E APARELHO PARA IMPEDIR A MANIPULAÇÃO DE PÁGINA WEB DE PAGAMENTO.

(51) Int.Cl.: G06F 21/00.

(30) Prioridade Unionista: 16/09/2011 CN 201110277604.7.

(73) Titular(es): TENCENT TECHNOLOGY (SHENZHEN) COMPANY LIMITED.

(72) Inventor(es): JIE LIN; WUSAN BAN; QIYUAN MENG.

(86) Pedido PCT: PCT CN2012081385 de 14/09/2012

(87) Publicação PCT: WO 2013/037304 de 21/03/2013

(85) Data do Início da Fase Nacional: 17/03/2014

(57) Resumo: APARELHO E MÉTODOS PARA IMPEDIR A MANIPULAÇÃO DE PÁGINA WEB DE PAGAMENTO. Aparelho refere-se a um aparelho e método para impedir a manipulação de página de pagamento que determinam se uma solicitação recebida por uma interface de modificação de página da Web é uma solicitação entre processos feita por outro processo diferente de um processo que executa a interface de modificação de página da Web e que, em resposta à determinação que a primeira solicitação é uma solicitação externa, interceptam a primeira solicitação. As modalidades do aparelho e método podem aumentar a segurança de transações de pagamento pela Internet.

Relatório Descritivo da Patente de Invenção para **"MÉTODO PARA IMPEDIR A MANIPULAÇÃO DE PÁGINA DA WEB E APARELHO PARA IMPEDIR A MANIPULAÇÃO DE PÁGINA WEB DE PAGAMENTO"**.

CAMPO DA INVENÇÃO

[001] A presente descrição refere-se geralmente a tecnologias de Internet, e mais particularmente, a um método e aparelho para impedir a manipulação de página da web de pagamento na Internet.

ANTECEDENTES DA INVENÇÃO

[002] À medida que as tecnologias de Internet continuam a se desenvolver, o comércio eletrônico (ou e-commerce) se tornou uma parte muito importante da Internet. Porém, questões de segurança e proteção em e-commerce contiveram as tecnologias de Internet contra o rápido desenvolvimento e implantação. Por exemplo, quando um usuário realiza um pagamento online através de uma página da Web de pagamento de navegador, a página da Web de pagamento pode ser manipulada por programas maliciosos como um programa Trojan, e o pagamento do usuário pode ser direcionado para uma parte ilegítima, fazendo com que o usuário sofra perdas econômicas.

[003] A Figura 1 mostra uma página web exemplificativa que permite que um usuário execute uma transação financeira através de banco online. A Figura 2 mostra uma página web exemplificativa que permite que um usuário confirme um pagamento através de banco online. Durante as transações de página da Web, um programa Trojan pode intervir e manipular as páginas da Web de pagamento em particular e redirecionar a solicitação de pagamento do usuário para páginas da Web de pagamento manipuladas, ilegítimas. O pagamento do usuário é, desse modo, realizado à parte ilegítima através da página da Web de pagamento manipulada pelo programa Trojan.

[004] Portanto, ainda há uma necessidade não atendida na técnica

para atender às deficiências e inadequações anteriormente mencionadas.

SUMÁRIO DA INVENÇÃO

[005] Alguns aspectos da presente descrição se referem a um método para impedir a manipulação de página de pagamento. O método inclui determinar se uma primeira solicitação recebida por uma interface de modificação de página da Web é uma solicitação externa, sendo que a solicitação externa é uma solicitação entre processos feita por um segundo processo diferente de um primeiro processo que executa a interface de modificação de página da Web, sendo que o primeiro processo é executado por um processador; e em resposta à determinação que a primeira solicitação é uma solicitação externa, intercepta a primeira solicitação.

[006] Alguns aspectos da presente descrição se referem a um aparelho para impedir a manipulação de página de pagamento. O aparelho inclui um detector de interface de modificação configurado para determinar se uma primeira solicitação recebida por uma interface de modificação de página da Web é uma solicitação externa, sendo que a solicitação externa é uma solicitação entre processos feita por um segundo processo diferente de um primeiro processo que executa a interface de modificação de página da Web; e um interceptador de solicitação configurado para, em resposta à determinação que a primeira solicitação é uma solicitação externa, intercepta a primeira solicitação.

[007] Alguns aspectos da presente descrição se referem a um meio legível por computador que armazena instruções que, quando executadas por um processador, fazem com que um computador realize um método para impedir a manipulação de página de pagamento. O método inclui determinar se uma primeira solicitação recebida por uma interface de modificação de página da Web é uma solicitação externa,

sendo que a solicitação externa é uma solicitação entre processos feita por um segundo processo diferente de um primeiro processo que executa a interface de modificação de página da Web; e em resposta à determinação que a primeira solicitação é uma solicitação externa, intercepta a primeira solicitação.

[008] Áreas adicionais de aplicabilidade da presente descrição se tornarão evidentes a partir da descrição detalhada fornecida a seguir. Deve ser entendido que a descrição detalhada e os exemplos específicos são destinados apenas para propósitos de ilustração e não pretendem limitar o escopo da descrição.

BREVE DESCRIÇÃO DOS DESENHOS

[009] Os desenhos em anexo ilustram uma ou mais modalidades da invenção e, juntamente com a descrição escrita, servem para explicar os princípios da invenção. Sempre que possível, referências numéricas similares serão usadas ao longo dos desenhos para se referirem a procedimentos iguais ou similares de uma modalidade. Os desenhos não limitam a presente invenção às modalidades específicas descritas e reveladas aqui. Os desenhos não são necessariamente representados em escala, em vez disso dá-se ênfase a ilustrar claramente os princípios da invenção. A presente descrição será mais completamente entendida a partir da descrição detalhada e dos desenhos em anexo, nos quais:

[0010] A Figura 1 mostra uma página da Web exemplificativa que permite que um usuário execute uma transação financeira através de banco online;

[0011] A Figura 2 mostra uma página da Web exemplificativa que permite que um usuário confirme um pagamento através de banco online;

[0012] A Figura 3 é um fluxograma que mostra um procedimento de proteção de acordo com algumas modalidades da presente descrição;

[0013] A Figura 4 é um fluxograma que mostra o procedimento de proteção de acordo com algumas modalidades da presente descrição;

[0014] A Figura 5 é um diagrama de bloco que mostra um aparelho que executa o procedimento de proteção de acordo com algumas modalidades da presente descrição; e

[0015] A Figura 6 é um diagrama de bloco que mostra um interceptador de solicitação do aparelho na Figura 5 de acordo com algumas modalidades da presente descrição.

DESCRIÇÃO DETALHADA DA INVENÇÃO

[0016] A seguinte descrição é meramente ilustrativa em natureza e não pretende limitar a descrição, sua aplicação ou usos. Os vastos ensinamentos da descrição podem ser implementados em uma variedade de formas. Portanto, embora essa descrição inclua exemplos particulares, o escopo da descrição não deve ser limitado visto que outras modificações se tornarão evidentes mediante um estudo dos desenhos, do relatório descritivo, e das concretizações seguintes. Para propósitos de clareza, referências numéricas similares serão usadas nos desenhos para identificar procedimentos ou componentes similares. Como usado aqui, a frase pelo menos um entre A, B, e C deve significar uma lógica (A ou B ou C), utilizando uma lógica não exclusiva OU. Deve ser entendido que uma ou mais etapas dentro de um método podem ser executadas em ordem diferente (ou simultaneamente) sem alterar os princípios da presente descrição.

[0017] Os termos usados nesse relatório descritivo geralmente possuem seus significados normais na técnica, dentro do contexto da descrição, e no contexto específico onde cada termo é usado. Alguns termos que são usados para descrever a descrição serão discutidos abaixo, ou ao longo do relatório descritivo, para fornecer instrução adicional ao profissional relativo à descrição. O uso de exemplos em algum lugar nesse relatório descritivo, inclusive exemplos de quaisquer

termos discutidos aqui, é apenas ilustrativo, e de forma alguma limita o escopo e significado da descrição ou de qualquer termo exemplificado. Também, a descrição não é limitada a várias modalidades fornecidas nesse relatório descritivo.

[0018] Como usado na descrição aqui e ao longo das concretizações que se seguem, o significado de "um", "uma", e "o" inclui referências no plural, exceto onde o contexto sugerir em contrário. Também, como usado na descrição aqui e ao longo das concretizações que se seguem, o significado de "em" inclui "em" e "sobre", exceto onde o contexto sugerir em contrário.

[0019] Como usado aqui, os termos "compreende," "inclui," "possui," "contém", "envolve," e similares serão entendidos como ilimitados, isto é, significam inclusive, porém não limitados a.

[0020] Como usado aqui, o termo módulo ou unidade pode se referir, ser parte, ou incluir um Circuito Integrado de Aplicação Específica (ASIC); um circuito eletrônico; um circuito de lógica combinatória; um arranjo de portas programável em campo (FPGA); um processador (compartilhado, dedicado, ou grupo) que executa um código; outros componentes de hardware adequados que proporcionam a funcionalidade descrita; ou uma combinação de alguns ou todos acima, como em um sistema em um chip. O termo módulo pode incluir uma memória (compartilhada, dedicada, ou grupo) que armazena um código executado pelo processador.

[0021] O termo código, como usado acima, pode incluir software, firmware, e/ou microcódigo, e pode se referir a programas, rotinas, funções, classes, e/ou objetos. O termo compartilhado, como usado acima, significa que alguns ou todos os códigos de múltiplos módulos podem ser executados utilizando um único processador (compartilhado). Ademais, alguns ou todos os códigos de múltiplos módulos podem ser armazenados por uma única memória

(compartilhada). O termo grupo, como usado acima, significa que alguns ou todos os códigos de um único módulo podem ser executados utilizando um grupo de processadores. Ademais, alguns ou todos os códigos de um único módulo podem ser armazenados utilizando um único grupo de memórias.

[0022] Os aparelhos e métodos descritos aqui podem ser implementados por um ou mais programas de computador executados por um ou mais processadores. Os programas de computador incluem instruções executáveis por processador que são armazenadas em um meio legível por computador tangível não temporário. Os programas de computador também podem incluir dados armazenados. Exemplos não limitativos do meio legível por computador tangível não temporário são memória não volátil, armazenamento magnético, e armazenamento óptico.

[0023] Em tecnologias de computador modernas, um navegador pode ser um componente sustentado por uma plataforma de um sistema de operação. Por exemplo, um MICROSOFT INTERNET EXPLORER é um componente sustentado pela plataforma de Modelo de Objeto Componente (COM) da MICROSOFT. Um processo de usuário pode criar um objeto INTERNET EXPLORER através de APIs de COM (Interfaces de Programação de Aplicativos) e bibliotecas. A plataforma COM fornece um mecanismo de comunicação, fazendo uso de pontos de conexão e depósitos, para suportar a comunicação entre um cliente COM e um servidor COM. Por exemplo, o cliente COM passa um ponto de conexão para o servidor COM. O servidor COM, mediante a ocorrência de alguns eventos, pode usar o ponto de conexão para passar mensagens para um depósito do cliente COM.

[0024] Um programa Trojan tipicamente é um código malicioso projetado principalmente para fornecer acesso a um hacker a arquivos de sistema de um computador do usuário. Isso proporciona aos hackers

a capacidade de mudar as configurações de arquivo, roubar arquivos ou senhas, danificar arquivos, monitorar atividades de usuário, ou executar processos que não são autorizados pelo usuário no computador do usuário.

[0025] Geralmente, quando um programa Trojan tenta modificar uma página de pagamento renderizada por um navegador (ou similarmente outro programa de aplicativo capaz de renderizar a página da Web), o programa Trojan será submetido às três seguintes etapas: (a) registrar o programa Trojan para receber eventos ou retornos de chamada do navegador renderizando a página de pagamento, (b) determinar se uma página renderizada pelo navegador é uma página de pagamento alvo que o programa Trojan pretende modificar, e (c) modificar a página de pagamento identificada na etapa (b). Uma página de pagamento se refere a uma exibição gráfica renderizada por um programa de aplicativo (por exemplo, uma página da Web renderizada por um navegador) que é usada por um usuário em execução de uma transação financeira online. Por exemplo, a página da Web mostrada na Figura 2 é uma página de pagamento e essa permite que um usuário do navegador transfira fundo da conta do usuário para outra parte. Exemplos de navegadores podem incluir qualquer navegador executável em um terminal de usuário como uma mesa de trabalho ou um dispositivo móvel, por exemplo, um navegador MICROSOFT INTERNET EXPLORE, um navegador FIREFOX, um navegador QQ, um navegador Chrome, ou um navegador Safari.

[0026] Dependendo das circunstâncias, a descrição abaixo pode usar o navegador MICROSOFT INTERNET EXPLORER como um exemplo para explicar as técnicas ou características da presente descrição. Um elemento versado na técnica poderia avaliar que essas técnicas ou características podem ser similarmente aplicadas a outros aplicativos de navegador ou aplicativos de Interface de Usuário. Quando

um usuário usa um navegador INTERNET EXPLORER para navegar na Internet, um programa Trojan instalado no computador pode monitorar o Localizador Uniforme de Recursos (URL) da página da Web que o usuário está acessando através do navegador INTERNET EXPLORER. O programa Trojan pode receber URLs, por exemplo, através de um evento BeforeNavigate2 gerado pelo navegador INTERNET EXPLORER. O programa Trojan então compara o URL da página da Web atual renderizada pelo navegador INTERNET EXPLORER ou os URLs contidos na página da Web atual com uma tabela ou lista de URLs de página da Web de pagamento conhecidos. Se os URLs atuais corresponderem a um URL de página de pagamento conhecido na tabela ou lista, o programa Trojan pode tentar modificar a página da Web através da função Write da interface IHTMLDocument 2, exibindo no navegador INTERNET EXPLORER uma página da Web manipulada que redireciona o pagamento do usuário para uma parte ilegítima fornecida pelo programa Trojan.

[0027] Ao manipular uma página de pagamento, o programa Trojan tipicamente utiliza as seguintes interfaces: (a) uma interface de registro de retorno de chamada através da qual um programa pode se registrar para receber eventos criados por um navegador que se referem à navegação do navegador, (b) uma interface de objeto de navegador através da qual um programa pode acessar as propriedades e funções do navegador, e (c) uma interface de modificação HTML através da qual um programa pode acessar uma página da Web particular renderizada pelo navegador e modificar o conteúdo da página da Web. Essas interfaces, através das quais o acesso e modificação a uma página da Web particular podem ser realizados, podem ser coletivamente referidas como interfaces de modificação de página da Web.

[0028] Um programa Trojan tipicamente é executado em um processo separado (ou diferente) de processos de navegador. Uma

solicitação do processo Trojan realizada para o processo de navegador é, desse modo, tipicamente uma solicitação entre processos ou uma solicitação externa. Algumas modalidades da presente descrição monitoram as solicitações entre processos ou solicitações externas para acessar o processo de navegador. Pode não ser necessário identificar a fonte da solicitação externa, isto é, determinar se a solicitação é resultante do processo Trojan; todas as solicitações externas ou solicitações entre processos para acessar o processo de navegador podem ser interceptadas.

[0029] Algumas modalidades da presente descrição implementam um procedimento de proteção que impede que um programa Trojan manipule uma página de pagamento (por exemplo, uma página da Web de banco online) renderizada por um navegador. Para determinar se uma chamada entre processos foi feita para o processo de navegador, o procedimento de proteção pode determinar inicialmente se a pilha de chamadas de um programa que implementa a interface de modificação de página da Web descrita acima contém um arquivo, procedimento, rotina, ou qualquer programa que implementa ou se refere a uma chamada de procedimento remoto (RPC). Se a pilha de chamadas desse programa contiver um arquivo relacionado à chamada RPC, o procedimento de proteção pode determinar que ocorreu uma solicitação entre processos para acessar a interface de modificação de página da Web. Por exemplo, em um ambiente COM, o procedimento de proteção determina se há um arquivo RPCRT4.dll em uma ou mais pilhas de chamadas de uma interface de gabinete de um gabinete que sustenta um objeto de navegador, uma interface de objeto de navegador, e uma interface de modificação HTML através da qual um programa pode modificar uma página da Web HTML particular do navegador. Mais particularmente, essas pilhas de chamadas podem incluir as pilhas de chamadas de programas que implementam as interfaces

IHTMLDocument2, IConnectionPointContainer ou IConnectionPoint, e IWebBrowser2. Por exemplo, uma única exibição de página da Web do navegador pode implementar a interface IHTMLDocument2; um módulo de gabinete COM pode implementar a interface IConnectionPointContainer; um módulo de ponto de conexão COM pode implementar a interface IConnectionPoint; e um navegador INTERNET EXPLORER pode implementar a interface IWebBrowser2. Nesse exemplo, se o arquivo RPCRT4.dll estiver em um ou mais dessas pilhas de chamadas, pode ser determinado que a solicitação recebida feita à interface de gabinete descrita acima, a interface de objeto de navegador, ou a interface de modificação HTML é uma solicitação externa ou entre processos.

[0030] Há muitos tipos de solicitações externas ou entre processos. Por exemplo, para manipular uma página de pagamento em um ambiente COM, um programa Trojan tipicamente precisa acessar: (a) uma função da interface de registro de retorno de chamada que permita que o programa Trojan se registre para receber eventos ou retornos de chamada do navegador; (b) uma função de obtenção de URL local da interface de objeto de navegador que retorna o URL da página da Web atualmente renderizada pelo navegador; e (c) uma função da interface de modificação HTML que é usada para fornecer o conteúdo da página que está sendo renderizada pelo navegador. Alguns exemplos específicos dessas funções incluem a função Advise da interface IConnectionPoint, a função GetLocationURL da interface IWebBrowser2, e a função Write da interface IHTMLDocument2.

[0031] A Figura 3 é um fluxograma que mostra um procedimento de proteção de acordo com algumas modalidades da presente descrição. Na operação 301, o procedimento de proteção determina se a solicitação feita ao processo de navegador é uma solicitação externa. Na operação 302, o procedimento de proteção intercepta a solicitação

externa feita ao processo de navegador. A solicitação externa pode ser uma solicitação entre processos enviada por um processo diferente daquele do navegador.

[0032] Um navegador pode renderizar várias páginas da Web. O procedimento de proteção pode ser adaptado para proteger vários tipos de páginas da Web renderizadas pelo navegador. Em algumas modalidades, o procedimento de proteção envolve impedir o pagamento não autorizado através de páginas da Web de pagamento manipuladas. Se o procedimento de proteção determinar que a página da Web atual renderizada pelo navegador não é uma página da Web de pagamento ou que as solicitações externas recebidas não estão relacionadas a nenhuma página da Web de pagamento, o procedimento de proteção pode escolher não interceptar essas solicitações externas.

[0033] Com isso, na operação 301, o procedimento de proteção também pode determinar se a página da Web renderizada pelo navegador é uma página da Web de pagamento.

[0034] Em algumas modalidades, o procedimento de proteção examina o URL de uma página da Web para determinar se a página da Web é uma página de pagamento. Os URLs de páginas de pagamento conhecidas podem ser armazenados como uma tabela ou uma lista no computador local que executa o procedimento de proteção ou em um dispositivo de armazenamento de rede. Como um exemplo ilustrativo, o seguinte URL é um URL de uma página da Web de pagamento. O URL é:

`<https://netpay.cmbchina.com/netpayment/BaseHttp.dll>.`

Essa página da Web de pagamento também contém links de URL de pagamento como:

`<rule host="https://netpay.cmbchina.com" path="/netpayment/BaseHttp.dll?PrePayC*" level="3"/>`

[0035] O procedimento de proteção pode, para determinar se a

página da Web é uma página de pagamento, comparar o URL mencionado acima da página da Web e os links contidos na página da Web com os URLs armazenados e/ou determinar se o URL e os links contêm as características definidoras de página de pagamento. As características definidoras podem ser predeterminadas e armazenadas na tabela ou lista de URL do sistema de computador.

[0036] A Figura 4 é um fluxograma que mostra o procedimento de proteção de acordo com algumas modalidades da presente descrição. Para impedir a manipulação de página da Web de pagamento, uma ou mais das seguintes operações podem ser realizadas: operação 401 para impedir que um programa Trojan se registre para receber retornos de chamada de evento de navegador; operação 402 para impedir que um programa Trojan obtenha a localização ou o URL de uma página da Web; e operação 403 para impedir que um programa Trojan modifique o conteúdo da página da Web.

[0037] Em algumas modalidades, a operação 403 pode ser combinada com a operação 401 e a operação 402. Essas operações não são necessariamente executadas nas sequências listadas acima.

[0038] Em algumas modalidades, a operação 401 pode impedir que programas maliciosos como um programa Trojan obtenham informações do navegador ou funções de chamada do navegador. Para monitorar os eventos do navegador, o programa Trojan tipicamente precisa chamar a interface de registro de retorno de chamada para se registrar de modo a receber eventos de navegador. Por exemplo, em um ambiente COM, o programa Trojan precisa chamar as funções Advise de objetos de ponto de conexão que implementam a interface IConnectionPoint sustentada pelos objetos de navegador ou objetos auxiliares de navegador para sinalizar que o programa Trojan está interessado em receber retornos de chamada ou eventos do navegador. Se as chamadas realizadas para a interface de registro de retorno de

chamada forem interceptadas, então o programa Trojan não será capaz de obter as informações de evento de navegador. Sem as informações de evento de navegador, o programa Trojan não será capaz de modificar a página da Web.

[0039] A operação 402 pode impedir que um programa malicioso como o programa Trojan obtenha a localização ou o URL da página renderizada pelo navegador (por exemplo, o URL local mostrado na barra de endereço do navegador). Normalmente o programa Trojan precisa ter esse URL para determinar se a página que está sendo renderizada pelo navegador é uma página de pagamento. O programa Trojan geralmente recebe múltiplos URLs de um retorno de chamada de evento de navegador. Por exemplo, se uma página da Web contiver quadros, o programa Trojan irá receber múltiplos URLs do evento de navegador. O programa Trojan deve chamar uma função da interface de objeto de navegador para obter o URL da página que está sendo atualmente renderizada pelo navegador, e usar o URL para determinar se a página atual é uma página de pagamento. Em um ambiente COM, o programa Trojan chama a função `GetLocationURL` da interface `IWebBrowser2` para obter esse URL. Na operação 402, o procedimento de proteção intercepta as chamadas feitas pelo programa Trojan para essa função da interface de objeto de navegador. Assim, o programa Trojan não será capaz de determinar se a página atual é uma página de pagamento com base no URL da página.

[0040] A operação 403 pode impedir que um programa malicioso como um programa Trojan modifique o conteúdo de uma página da Web. O programa Trojan eventualmente precisa chamar uma interface de modificação HTML para modificar a página de pagamento que está sendo renderizada pelo navegador. Em um ambiente COM, o programa Trojan chama a função `Write` da interface `IHTMLDocument2` para modificar o conteúdo da página da Web. Na operação 403, o

procedimento de proteção pode interceptar as chamadas feitas pelo programa Trojan para essa função da interface de modificação HTML. Assim, o procedimento de proteção impede que o programa Trojan modifique o conteúdo da página renderizada pelo navegador.

[0041] Em algumas modalidades, quando se executa uma ou mais operações 401-403, como discutido acima, o procedimento de proteção também pode determinar se a solicitação atual é uma solicitação entre processos ou externa. Em um ambiente COM, o procedimento de proteção verifica as pilhas de chamadas de programas que implementam as interfaces IHTMLDocument2, IConnectionPointContainer, IConnectionPoint, e IWebBrowser2. Geralmente, se essas pilhas de chamadas contiverem um arquivo relacionado à RPC como RPCRT4.dll, o procedimento de proteção pode determinar que uma solicitação atual feita para as interfaces acima é uma solicitação entre processos ou externa. A interceptação dessa solicitação entre processos ou externa pode impedir que o programa Trojan acesse a interface de gabinete, a interface de objeto de navegador, e a interface de modificação HTML descritas acima.

[0042] O procedimento de proteção pode ser implementado no mesmo computador em que o navegador está sendo executado. O procedimento de proteção pode ser executado em um processo executado por um processador (por exemplo, uma CPU) do computador. O processo do procedimento de proteção pode ser igual ao processo de navegador. Por exemplo, o procedimento de proteção pode ser implementado como um programa de extensão do navegador. O processo do procedimento de proteção pode ser alternativamente um processo independente e separado do processo de navegador.

[0043] A Figura 5 é um diagrama de bloco que mostra um aparelho que executa o procedimento de proteção de acordo com algumas modalidades da presente descrição. O aparelho 50 inclui: (a) um

detector de interface de modificação 51 configurado para detectar se uma solicitação ou chamada recebida pela interface de modificação de página da Web é uma solicitação externa, e (b) um interceptador de solicitação 52 configurado para interceptar a solicitação externa quando a solicitação externa for detectada pelo detector de interface de modificação 51. A solicitação externa pode ser uma solicitação entre processos de um processo diferente de um processo de página da Web atualmente executado. O detector de interface de modificação 51 e o interceptador de solicitação 52 podem ser módulos físicos e/ou lógicos que empregam ou utilizam hardware necessário (por exemplo, um processador e uma memória) e software para implementar as características desejadas.

[0044] A interface de modificação de página da Web inclui a interface de registro de retorno de chamada de um programa para se registrar de modo a receber retornos de chamada ou notificações de eventos de navegador referentes à modificação de uma página de pagamento, a interface de objeto de navegador, e uma ou mais interfaces de modificação HTML. Consequentemente, a solicitação externa descrita acima inclui chamadas feitas para a função `advise` da interface de registro de retorno de chamada, a função de obtenção de URL local da interface de objeto de navegador, e uma ou mais funções `write` da interface de modificação HTML. A função `advise` da interface de registro de retorno de chamada permite que um programa se registre para receber eventos ou retornos de chamada do navegador. A função de obtenção de URL local da interface de objeto de navegador permite que um programa recupere o URL da página da Web que o objeto de navegador está atualmente renderizando, que é geralmente o URL mostrado na barra de endereço do navegador. A função `write` da interface de modificação HTML permite que um programa forneça o conteúdo que será renderizado pelo navegador. Em um ambiente COM,

um exemplo da função `advise` da interface de registro de retorno de chamada é a função `Advise` da interface `IConnectionPoint`. Um exemplo da função de obtenção de URL local é a função `GetLocationURL` da interface `IWebBrowser2`. Um exemplo da função `write` da interface de modificação HTML é a função `Write` da interface `IHTMLDocument2`.

[0045] Em algumas modalidades, o detector de interface de modificação 51 também pode ser usado para determinar se a pilha de chamadas de um processo que executa a interface de modificação de página da Web contém um arquivo relacionado à RPC (como o arquivo `RT4.dll`). Quando o detector de interface de modificação 51 determinar que a pilha de chamadas contém esse arquivo, então esse determina que a interface de modificação de página da Web recebeu uma solicitação externa. O detector de interface de modificação 51 também pode ser usado para determinar se a página atual renderizada pelo navegador é uma página de pagamento.

[0046] A Figura 6 é um diagrama de bloco que mostra um interceptador de solicitação 52 do aparelho de acordo com algumas modalidades da presente descrição. O interceptador de solicitação 52 pode incluir pelo menos uma entre: (a) uma unidade de interceptação de informações 620 configurada para interceptar as chamadas ou solicitações de outro processo feitas para a função `advise` da interface de registro de retorno de chamada (como a função `Advise` da interface `IConnectionPoint`) para obter informações de navegador; (b) uma unidade de interceptação de determinação 622 configurada para interceptar as chamadas ou solicitações de outro processo feitas para a função de obtenção de URL local da interface de objeto de navegador (como a função `GetLocationURL` da interface `IWebBrowser2`) para determinar se a página atual é uma página de pagamento; e (c) uma unidade de interceptação de modificação 624 configurada para interceptar as chamadas ou solicitações de outro processo feitas para a

função write da interface de modificação HTML (como a função Write da interface IHTMLDocument2) para modificar o conteúdo de uma página de pagamento.

[0047] Algumas modalidades da presente descrição podem impedir efetivamente a manipulação de página da Web de pagamento por um programa Trojan. Por exemplo, as solicitações externas de um programa malicioso como um programa Trojan que tenta manipular uma página da Web de pagamento podem ser distinguidas, detectadas e interceptadas por algumas modalidades da presente descrição. Algumas modalidades podem aumentar a segurança e proteção de transações bancárias online e de pagamento eletrônico.

[0048] Como é entendido pelo elemento versado na técnica, partes ou todas as características da presente descrição podem ser implementadas por programas de computador executados por hardware de computador relacionado que inclui um processador. A presente descrição pode ser armazenada em um meio legível/gravável de computador, que inclui disco magnético, CD/DVD, Memória de Leitura ou ROM, e Memória de Acesso Aleatório ou RAM.

[0049] A descrição anterior das modalidades exemplificativa da invenção foi apresentada apenas para os propósitos de ilustração e descrição e não pretende ser exaustiva ou limitar a invenção às formas precisas descritas. Muitas modificações e variações são possíveis devido à instrução acima.

[0050] As modalidades foram selecionadas e descritas para explicar os princípios da invenção e sua aplicação prática para estimular outros elementos versados na técnica a utilizarem a invenção e várias modalidades e com várias modificações adequadas ao uso particular contemplado. Modalidades alternativas se tornarão evidentes para os elementos versados na técnica às quais a presente invenção pertence sem que se abandone seu espírito e escopo. Consequentemente, o

escopo da presente invenção é definido pelas concretizações em anexo em vez da descrição anterior e das modalidades exemplificativas descritas nessa.

REIVINDICAÇÕES

1. Método para impedir a manipulação de página da Web, **caracterizado pelo fato de que** o método compreende as etapas de:

determinar (301) se uma primeira solicitação recebida por uma interface de modificação de página da Web é uma solicitação externa, a solicitação externa sendo uma solicitação entre processos feita por um segundo processo diferente de um primeiro processo que executa a interface de modificação de página da Web, o primeiro processo sendo executado por um processador; e

em resposta à determinação que a primeira solicitação é uma solicitação externa, interceptar (302) a primeira solicitação;

em que a interface de modificação de página de Web compreende uma interface de modificação HTML, a solicitação externa compreende uma solicitação feita para uma função Write da interface de modificação HTML, e a função Write da interface de modificação HTML permite que um programa forneça um conteúdo a ser renderizado para um navegador e compreende uma função Write de uma interface IHTMLDocument2; e

interceptar (302) a primeira solicitação compreende a etapa de:

interceptar uma chamada feita do segundo processo para a função Write da interface de modificação HTML pra modificar um conteúdo de uma página de Web que está atualmente rederizada pelo navegador.

2. Método, de acordo com a reivindicação 1, **caracterizado pelo fato de que** a interface de modificação de página da Web ainda compreende pelo menos uma entre uma interface de registro de retorno de chamada que permite que um programa se registre para receber retornos de chamada ou eventos do navegador e referente à modificação da página da Web, e uma interface de objeto de navegador.

3. Método, de acordo com a reivindicação 2, **caracterizado pelo fato de que** a solicitação externa ainda compreende uma solicitação feita para uma função advise da interface de registro de retorno de chamada, ou uma função de obtenção de URL local da interface de objeto de navegador,

em que a função advise da interface de registro de retorno de chamada permite que um programa se registre para receber os retornos de chamada ou eventos do navegador, e a função de obtenção de URL local da interface de objeto de navegador permite que um programa recupere o URL da página da Web.

4. Método, de acordo com a reivindicação 3, **caracterizado pelo fato de que** a função advise da interface de registro de retorno de chamada compreende uma função Advise de uma interface IConnectionPoint, e a função de obtenção de URL local da interface de objeto de navegador compreende uma função GetLocationURL de uma interface IWebBrowser2.

5. Método, de acordo com a reivindicação 3, **caracterizado pelo fato de que** a etapa de interceptar (302) a primeira solicitação compreende pelo menos um entre

interceptar uma chamada realizada do segundo processo para a função advise da interface de registro de retorno de chamada para obter informações de navegador; e

interceptar uma chamada realizada do segundo processo para a função de obtenção de URL local da interface de objeto de navegador para determinar se uma página atualmente renderizada por um navegador é uma página de pagamento.

6. Método, de acordo com a reivindicação 1, **caracterizado pelo fato de que** a etapa de determinar (301) se a primeira solicitação recebida pela interface de modificação de página da Web é uma solicitação externa compreende

determinar se uma pilha de chamadas da interface de modificação de página da Web contém um arquivo relacionado à chamada de procedimento remoto (RPC); e

determinar, em resposta à determinação que a pilha de chamadas contém um arquivo relacionado à RPC, que a primeira solicitação recebida pela interface de modificação de página da Web é uma solicitação externa.

7. Método, de acordo com a reivindicação 6, **caracterizado pelo fato de que** o arquivo relacionado à RPC inclui arquivo RPCRT4.dll.

8. Método, de acordo com a reivindicação 1, **caracterizado pelo fato de que** ainda compreende a etapa de determinar se uma página que está sendo atualmente renderizada por um navegador é uma página de pagamento ao comparar um URL da página com as características definidoras predeterminadas de URLs de páginas da Web de pagamento.

9. Aparelho para impedir a manipulação de página de pagamento (50), **caracterizado pelo fato de que** o aparelho compreende:

um detector de interface de modificação (51) configurado para determinar se uma primeira solicitação recebida por uma interface de modificação de página da Web é uma solicitação externa, sendo que a solicitação externa é uma solicitação entre processos feita por um segundo processo diferente de um primeiro processo que executa a interface de modificação de página da Web; e

um interceptador de solicitação (52) configurado para, em resposta à determinação que a primeira solicitação é uma solicitação externa, interceptar a primeira solicitação;

em que a interface de modificação de página de Web compreende uma interface de modificação HTML, a solicitação externa

compreende uma solicitação feita para uma função Write da interface de modificação HTML, e a função Write da interface de modificação HTML permite que um programa forneça um conteúdo a ser renderizado para um navegador e compreende uma função Write de uma interface IHTMLDocument2; e

uma unidade de interceptação de modificação (624) configurada para uma chamada feita do segundo processo para a função Write da interface de modificação HTML pra modificar um conteúdo de uma página de Web que está atualmente rederizada pelo navegador.

10. Aparelho (50), de acordo com a reivindicação 9, **caracterizado pelo fato de que** a interface de modificação de página da Web ainda compreende pelo menos um dentre uma interface de registro de retorno de chamada que é configurada para permitir que um programa se registre para receber os retornos de chamada ou eventos do navegador e referente à modificação da página da Web, e uma interface de objeto de navegador, e

em que a solicitação externa ainda compreende uma solicitação feita para uma função advise da interface de registro de retorno de chamada, ou uma função de obtenção de URL local da interface de objeto de navegador,

em que a função advise da interface de registro de retorno de chamada é configurada para permitir que um programa se registre para receber os retornos de chamada ou eventos do navegador, e a função de obtenção de URL local da interface de objeto de navegador é configurada para permitir que um programa recupere o URL da página da Web.

11. Aparelho (50), de acordo com a reivindicação 10, **caracterizado pelo fato de que** a função advise da interface de registro de retorno de chamada compreende uma função Advise de uma

interface IConnectionPoint, e a função de obtenção de URL local da interface de objeto de navegador compreende uma função GetLocationURL de uma interface IWebBrowser2.

12. Aparelho (50), de acordo com a reivindicação 10, **caracterizado pelo fato de que** o interceptador de solicitação (52) compreende:

uma unidade de interceptação de informações (620) configurada para interceptar uma chamada realizada do segundo processo para a função advise da interface de registro de retorno de chamada para obter informações de navegador; e

uma unidade de interceptação de determinação (622) configurada para interceptar uma chamada realizada do segundo processo para a função de obtenção de URL local da interface de objeto de navegador para determinar se uma página atualmente renderizada por um navegador é uma página de pagamento.

13. Aparelho (50), de acordo com a reivindicação 9, **caracterizado pelo fato de que** o detector de interface de modificação (51) é ainda configurado para

determinar se uma pilha de chamadas da interface de modificação de página da Web contém um arquivo RPCRT4.dll, e

determinar, em resposta à determinação que a pilha de chamadas contém um arquivo RPCRT4.dll, que a primeira solicitação recebida pela interface de modificação de página da Web é uma solicitação externa.

14. Aparelho (50), de acordo com a reivindicação 9, **caracterizado pelo fato de que** o detector de interface de modificação (51) é ainda configurado para determinar se uma página atualmente sendo renderizada por um navegador é uma página de pagamento ao comparar um URL da página com as características definidoras predeterminadas de URLs de páginas da Web de pagamento.

15. Meio legível por computador que armazena instruções **caracterizado pelo fato de que** as instruções, quando executadas por um a processador, fazem com que um computador realize um método para impedir a manipulação de página de pagamento, sendo que o método compreende as etapas de:

determinar se uma primeira solicitação recebida por uma interface de modificação de página da Web é uma solicitação externa, a solicitação externa sendo uma solicitação entre processos feita por um segundo processo diferente de um primeiro processo que executa a interface de modificação de página da Web, o primeiro processo sendo executado por um processador; e

em resposta à determinação que a primeira solicitação é uma solicitação externa, interceptar a primeira solicitação;

em que a interface de modificação de página de Web compreende uma interface de modificação HTML, a solicitação externa compreende uma solicitação feita para uma função write da interface de modificação HTML, e a função Write da interface de modificação HTML permite que um programa forneça um conteúdo a ser renderizado para um navegador e compreende uma função Write de uma interface IHTMLDocument2; e

interceptar a primeira solicitação compreende a etapa de:

interceptar uma chamada feita do segundo processo para a função write da interface de modificação HTML pra modificar um conteúdo de uma página de Web que está atualmente rederizada pelo navegador.

1. Confirm Order → 2. Pay to Alipay → 3. Seller Shipping, Buyer Confirm → 4. Alipay to Seller → 5. Raking

Order

Fan, Dexi ... Detail

Receiving

Ni, Yongquan

online services

Your Account : 15801187521

Available amount : 0.00

You May Choose : Saving Credit

Please choose your payment

Online Banking : ☒ Bank 1 ☐ Bank 2 ☐ Bank 3 ☐ Bank 4

☐ Bank 5 ☐ Bank 6 ☐ Bank 7 ☐ Bank 8

☐ Bank 9 ☐ Bank 10 ☐ Bank 11 ☐ Bank 12

☐ Bank 13 ☐ Bank 14 ☐ Bank 15 ☐ Bank 16

FIG. 1



FIG. 2

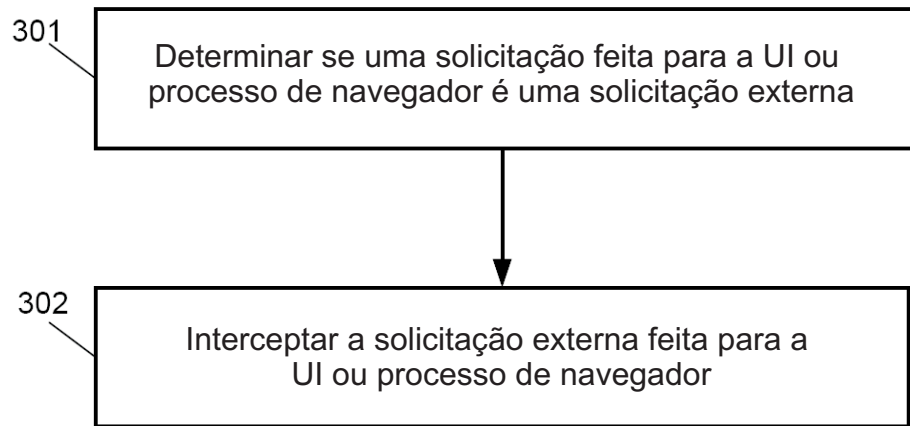


FIG. 3

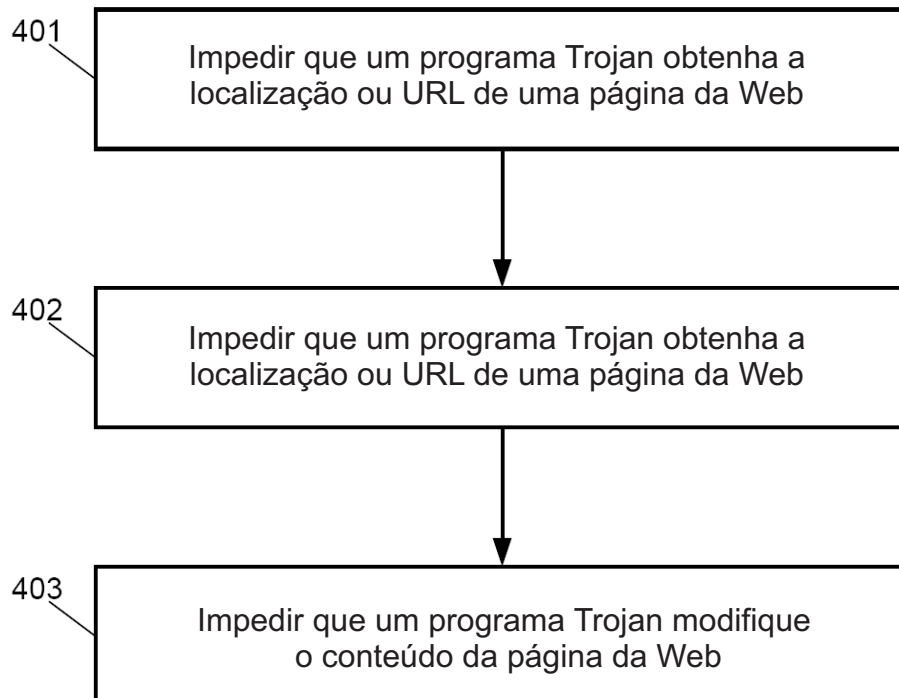


FIG. 4

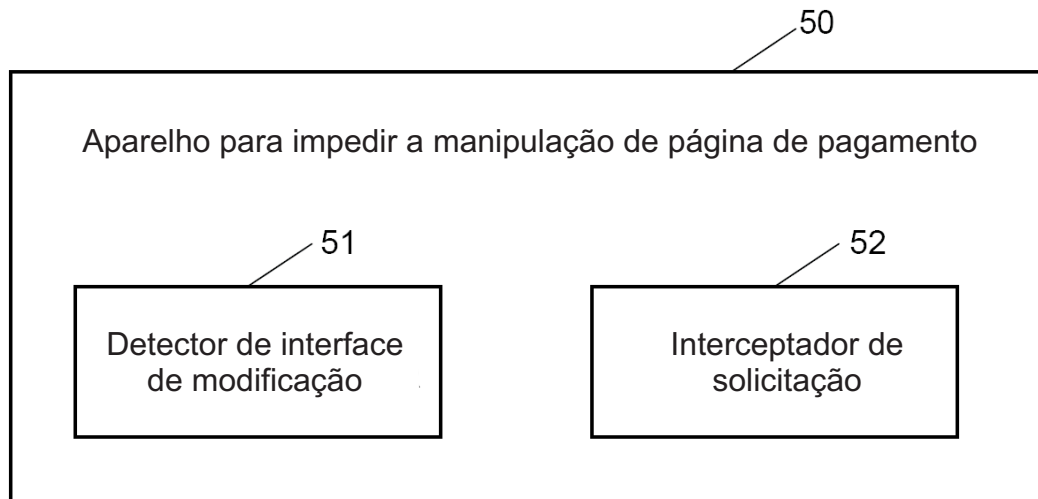


FIG. 5

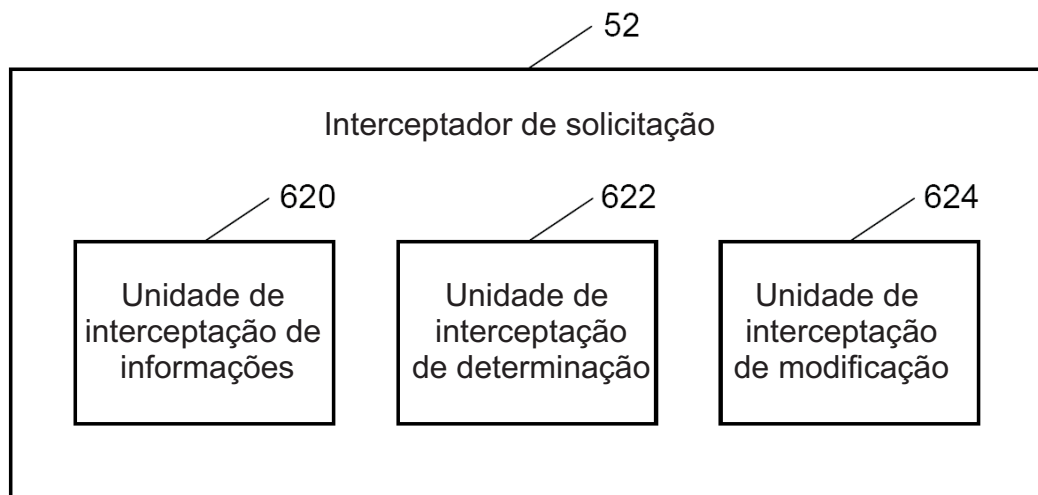


FIG. 6