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

(11) PI 0608276-9 B1

(22) Data do Depósito: 20/02/2006

(45) Data de Concessão: 05/02/2019

(54) Título: MÉTODO E SISTEMA PARA MAPEAR UM PACOTE DE SOLICITAÇÃO DE REDE CRIPTOGRAFADO PARA SUA CÓPIA DESCRIPTOGRAFADA EM UM SERVIDOR DA WEB DA REDE DE COMPUTADOR SEGURO

(51) Int.Cl.: H04L 29/08.

(52) CPC: H04L 63/0428; H04L 63/1425; H04L 63/168; H04L 67/02.

(30) Prioridade Unionista: 28/02/2005 US 11/067,990.

(73) Titular(es): INTERNATIONAL BUSINESS MACHINES CORPORATION.

(72) Inventor(es): PAUL FREDRIC KLEIN; JESSE NICHOLAS PEREZ.

(86) Pedido PCT: PCT EP2006060107 de 20/02/2006

(87) Publicação PCT: WO 2006/089879 de 31/08/2006

(85) Data do Início da Fase Nacional: 28/08/2007

(57) Resumo: MAPEAMENTO DE PACOTE DE REDE DE HTTPS CRIPTOGRAFADO PARA UM NOME DE URL ESPECÍFICO E OUTROS DADOS SEM DESCRIPTOGRAFAÇÃO FORA DE UM SERVIDOR DA WEB SEGURO. Um sistema e um método baseado em computador de mapeamento de pacote de solicitação de rede criptografado para sua cópia descriptografada em um servidor da web seguro da rede de computador. O método cria um módulo plug-ín em um servidor da web seguro e salva pelo menos um endereço de rede e o número de porta de um pacote de solicitação de rede criptografado capturado. O módulo plug-in obtém uma cópia descriptografada do pacote da solicitação de rede a partir do módulo seguro de descriptografação do servidor da web e retorna a mesma com o endereço de rede e o número de porta.

"MÉTODO E SISTEMA PARA MAPEAR UM PACOTE DE SOLICITAÇÃO DE REDE CRIPTOGRAFADO PARA SUA CÓPIA DESCRIPTOGRAFADA EM UM SERVIDOR DA WEB DA REDE DE COMPUTADOR SEGURO"

Campo da Invenção

[0001] Esta invenção relaciona-se, de modo geral, ao campo de redes de computadores, e especialmente a um método e a um sistema para mapeamento altamente eficiente de pacotes de rede de HTTPS criptografados para um nome de URL específico e a outros dados criptografados sem executar a descriptografia fora de um servidor da web seguro.

Antecedentes da Invenção

[0002] A Internet é uma rede vasta de computadores heterogêneos e de sub-redes que se comunicam em conjunto para permitir a troca de informação global. O *World Wide Web* (WWW) é um dos serviços de informação mais populares na Internet que usa o software navegador da web para decifrar as ligações de hipertexto para os documentos e arquivos situados em computadores remotos ou em servidores de conteúdo para alcançar a informação multimídia na forma de texto, áudio, vídeo, gráfico, animação, figuras estáticas, etc. Tornou-se cada vez mais necessário que os usuários acessem remotamente redes públicas e privadas e um problema surge sobre como permitir um acesso seguro aos recursos disponíveis em servidores seguros e as redes através de uma rede pública geralmente insegura, tal como a Internet.

[0003] Muitos utilitários de software e hardware e aplicativos, tais como monitores de desempenho da rede, têm como sua tecnologia principal um método de medição que depende dos dados da rede como sua entrada. Como cada vez

mais comércio eletrônico aparece na Internet, o uso de transportes de rede seguros aumenta. A criptografia pelos navegadores da web é a única fonte mais usada de envio de dados seguros através da Internet por meio do protocolo de transferência de hipertexto seguro (HTTPS). Para o protocolo de HTTPS, um navegador da web usa tecnologia de chave pública/privada que criptografa os dados da rede tão fortemente que somente um servidor da web seguro correspondente pode descriptografar a mesma. É virtualmente impossível para um hardware ou monitor de software, que tem acesso a estes fluxos de rede criptografados, para compreender qualquer coisa sobre seus formatos, deixando de lado qualquer coisa sobre seus conteúdos. Por causa desta limitação das ferramentas de monitoração em um ambiente de HTTPS, o valor dos dados para os monitores de hardware e software desta rede podem somente ser realizados para ambientes usando o HTTP, que é a versão não segura de HTTPS. Além disso, se a descriptografia for feita fora do servidor da web seguro, isso requer um software especial de descriptografia regulado pelo governo que o torna menos atrativo ao marketing e à distribuição. É também menos atrativo aos clientes porque requer acesso aos certificados de segurança do servidor da web, que os clientes não permitiriam. É, consequentemente, importante usar uma outra técnica que seja mais tolerável às regulamentações do governo, ao mercado e aos clientes.

[0004] Consequentemente, existe uma necessidade de um método e de um sistema simples, otimizado e genérico que use servidores seguros da rede para descriptografar uma

porção dos dados da rede para permitir que monitores de rede de hardware e de software obtenham a informação que necessitam para operar de modo que possam retornar os mesmos dados como se em operação no ambiente de http não seguro, sem usar um software especial de descriptografia fora de um servidor seguro da rede.

Descrição da Invenção

[0005] Os objetivos, características, e vantagens precedentes e outros, da presente invenção tornar-se-ão aparentes a partir da seguinte descrição detalhada das concretizações preferidas, que fazem referência a diversas figuras.

[0006] Uma concretização preferida da presente invenção é um método para mapear um pacote de solicitação de rede criptografado para sua cópia descriptografada em um servidor da web de rede de computador seguro. O método cria um módulo plug-in em um servidor da web seguro e salva pelo menos um endereço de rede e o número da porta de um pacote de solicitação de rede criptografado capturado. O módulo plug-in obtém uma cópia descriptografada do pacote da solicitação de rede do módulo de descriptografia do servidor da web seguro e retorna a mesma com o endereço de rede e o número da porta.

[0007] Uma outra concretização preferida da presente invenção é um sistema que executa as concretizações acima mencionadas do método da presente invenção.

[0008] Contudo, uma outra concretização preferida da presente invenção inclui uma mídia utilizável por computador que concretiza tangivelmente um programa de instruções

executáveis pelo computador para executar as etapas de método das concretizações acima mencionadas do método da presente invenção.

Breve Descrição dos Desenhos

[0009] Fazendo referência agora aos desenhos, em que números de referência semelhantes representam partes correspondentes durante toda a descrição:

A figura 1 ilustra um ambiente de rede de hardware e de software que permite mapeamento eficiente, de acordo com as concretizações preferidas da presente Invenção.

A figura 2 ilustra um fluxograma de nível superior do mapeamento, de acordo com as concretizações preferidas da presente invenção.

Descrição Detalhada das Concretizações Preferidas

[0010] Na seguinte descrição de concretizações preferidas, referência é feita aos desenhos anexos, em que formam parte da mesma, e em quais são mostrados, por meio de ilustração, as concretizações específicas em que a invenção pode ser praticada. Deve ser compreendida que outras concretizações podem ser utilizadas e alterações estruturais e funcionais podem ser feitas sem se afastar do escopo da presente invenção.

[0011] O objetivo principal da presente invenção é permitir que utilitários de rede dei hardware e software e aplicativos operarem em um ambiente seguro e tenham acesso aos mesmos dados como se em operação no ambiente de protocolo de transferência de hipertexto (HTTP) não seguro, e tenham a descriptografia dos dados da rede feita por um servidor da

web seguro, como parte da operação normal do servidor da web.

[0012] A presente invenção divulga um sistema, um método e uma mídia utilizável por computador que concretiza um programa de instruções executáveis por um computador para executar o método de mapeamento de um pacote de solicitação de rede criptografado para sua cópia descriptografada em um servidor seguro da rede de computadores. O módulo de monitoração da presente invenção obtém uma cópia descriptografada do pacote da solicitação de rede a partir do módulo de descriptografia do servidor da web seguro.

[0013] A solicitação de rede criptografada é preferivelmente uma solicitação de linguagem de marcação de hiperbexto (HTML) criptografada e seus dados criptografados, tal como o nome do localizador de recurso universal (URL), são necessários para alcançar um website. Para obter a informação criptografada fora de um pacote de solicitação de rede de HTTPS sem ter que executar uma tecnologia especial de descriptografia, a presente invenção emprega a habilidade de um servidor da web para ter um pacote da rede de HTTPS descriptografado entregue como parte do plug-in do servidor da web. Assim, a presente invenção não requer que a descriptografia ocorra fora de um servidor da web seguro. Além disso, não requer um software especial de descriptografia, mas utiliza os dados obtidos de um software de descriptografia convencional do servidor da web seguro durante sua operação normal. Desta maneira, a descriptografia é feita por um software convencional do

servidor da web já aprovado pelo governo, já aceito no mundo do marketing e distribuição e já em uso pelos clientes.

[0014] O aspecto principal da presente invenção mapeia uma solicitação de HTML completamente criptografada, como visto por um software de monitoramento de hardware ou software, para a solicitação de HTML completamente descriptografada, como visto por um servidor da web seguro. Isso pode ser realizado devido ao fato que todos os servidores da web seguros comercialmente usados fornecem uma técnica publicada para obter uma cópia do pacote de solicitação de HTML criptografado e para entregar, após a descriptografia, uma cópia do pacote de solicitação descriptografado para um monitor da presente invenção que normaliza os dados de modo que eles pareçam os dados obtidos de um ambiente de HTTP não seguro. O tipo da técnica publicada requerida para obter uma cópia descriptografada do pacote de solicitação de HTML depende do tipo do servidor da web seguro do vendedor que é usado pelo cliente.

[0015] A figura 1 ilustra um ambiente de rede de hardware e de software que permite o mapeamento eficiente, de acordo com as concretizações preferidas da presente invenção. O sistema usa o algoritmo para o mapeamento mostrado no fluxograma da figura 2. Em um diagrama de bloco da figura 1, um cliente em um local de cliente 100 interage com um local de servidor 200 que é preferivelmente seguro, através de uma rede 300. A rede 300 é geralmente a Internet usando o protocolo de controle de transmissão/ Protocolo de Internet (*Transmission Control Protocol/ Internet Protocol* - TCP/IP) que é o protocolo de comutação de pacote através

da Internet. O local de cliente 100 pode ser um computador desktop ou laptop, assistente digital pessoal (PDA), computador de bordo do veículo, telefone celular etc., que envia sua solicitação, tal como uma solicitação para um website, sob o protocolo de transferência de hipertexto (HTTP) ou sob o protocolo de transferência de hipertexto seguro (HTTPS) a um provedor de serviço da Internet (ISP), não mostrado. O ISP estabelece uma ligação com a Internet que passa então a solicitação para um servidor de conteúdo, não mostrado, que envia o pedido a um provedor de conteúdo, não mostrado, tipicamente endereçado pelo nome do localizador de recurso uniforme (URL).

[0016] A resposta do servidor de conteúdo é rateada de volta ao local de cliente 100 e é tipicamente condescendente com a linguagem de marcação de hipertexto (HTML), que é a linguagem padrão para criar documentos na WWW. O HTML define a estrutura e o layout de um documento da web que usa uma variedade dos comandos de tags introduzidos no documento para especificar como uma porção ou o documento inteiro devem ser formatados. Uma solicitação pode ser emitida para um servidor seguro, que é um servidor de conteúdo que suporta alguns dos principais protocolos de segurança que criptografam e descriptografam mensagens para as proteger contra falsificações de terceiros. Um protocolo típico é um protocolo de camada de soquetes seguro (SSL) que usa a criptografia com uma chave pública e privada e uma senha; outros métodos usam certificados digitais criptografados. O soquete de um SSL é tipicamente um objeto de software.

[0017] A unicidade da presente invenção encontra-se em mapear uma solicitação de HTML criptografado aleatória, capturada pelo hardware ou software de monitoração da rede, para o nome do URL e de outros dados criptografados que fornecem valor para o software de monitoração. Cada solicitação de HTTPS tem um cabeçalho pequeno, não criptografado que flui na rede como parte da solicitação e é ajustado apenas na frente da solicitação. Isto é necessário para dispositivos de rede, tais como roteadores e switches, para rotear uma solicitação para um endereço de rede de destino. Os dispositivos de rede não podem ler dados criptografados assim este cabeçalho deve permanecer descriptografado. Este cabeçalho é usado para vantagem desta invenção. Quando uma solicitação de HTML criptografada aleatória é capturada pelo software de monitoração da rede, seus endereços e portas de rede de origem e de destino são salvos em uma estrutura de dados em memória para um acesso posterior à solicitação criptografada.

[0018] O algoritmo para um procedimento de mapeamento exemplificativo é ilustrado por um fluxograma na figura 2. Nos aspectos preferidos da presente invenção, um usuário do local de cliente 100 usa o protocolo de HTTPS para criptografar seus pacotes da rede. Isto faz com que estes sejam ilegíveis às tecnologias que monitoram aos pacotes que atravessam a rede 300, tal como sniffers de pacote de rede, e somente um servidor da web com um protocolo de HTTPS correspondente pode criptografar os pacotes recebidos da rede. O usuário interage com o local de servidor 200 através de um navegador da web 110, situado no local de

cliente 100, que criptografa os pacotes da rede e posiciona uma solicitação de HTTPS na rede 300. A solicitação atravessa a rede 300 e chega ao servidor 200, onde um software de monitoração nomeado monitor 210 da presente invenção está em operação. O monitor 210 corresponde com um sniffer de pacote da rede 220 que está sempre em funcionamento. Assim, o monitor 210 vê o conteúdo criptografado do pacote da rede, mas não pode fazer muito sentido a partir dele. Entretanto, mesmo os pacotes criptografados da rede têm uma porção em um cabeçalho que não é criptografado, como o endereço de rede e o número de porta, que precisa permanecer descriptografado porque é usado pelos roteadores de hardware que não têm a capacidade de descriptografia. Consequentemente, o monitor 210 pode ler com sucesso o endereço de rede e o número da porta de pacotes de rede criptografados, mas nada mais. Entretanto, existe uma necessidade de os usuários lerem alguns dados que são embarcados no pacote de rede criptografado, tal como o nome do URL. Consequentemente, na etapa 400 da figura 1, o monitor 210 cria e registra um módulo plug-in 230 com um servidor da web 205 no momento em que o servidor da web 205 é iniciado.

[0019] A fim de executar o mapeamento entre o nome do URL e outros dados criptografados, e o número de endereço de rede do cliente e de porta, no monitor 210 de etapa 410 conserva o endereço de rede e o número de porta do pacote de solicitação de rede criptografado, originado no local de cliente 100 e recebido do sniffer de pacote de rede 220. O monitor 210 toma então uma cópia do pacote de rede criptografado e posiciona aquele pacote criptografado em uma

estrutura de dados 240 em uma memória 250. A estrutura de dados pode ser uma árvore relacionada ao URL da raiz específica ou a uma tabela ou fila indexada pelo endereço de rede e pelo número de porta do local do cliente.

[0020] No servidor da web 205, o pacote da rede é descriptografado pelo software de descriptografia do servidor da web convencional 225, situado dentro do servidor da web 205, como parte do processamento normal do servidor da web. O módulo plug-in 230 é tipicamente referido como um filtro da web, para servidores da web Microsoft IIS, e um NSAPI, para servidores da web do Apache e Netscape. Na etapa 420, o módulo plug-in 230 obtém as cópias dos pacotes de rede de HTTPS a partir da solicitação de HTML descriptografada.

[0021] Uma vez que o módulo plug-in 230 obtém a cópia descriptografada dos pacotes de rede de HTTPS do software de descriptografia do servidor da web convencional 225, os dados importantes, tais como o nome do URL, a referência do URL e o conteúdo específico do pedido podem ser extraídos desta cópia da solicitação. Entretanto, desde que somente uma cópia da solicitação de HTML foi obtida pelo filtro da web ou NSAPI, a informação específica da rede não está disponível e essa informação é o que é necessário para fazer uma correspondência de relação para o pedido criptografado original. Consequentemente, algumas interfaces do programa de aplicação (APIs) têm que ser invocadas no servidor da web seguro para obter o endereço de rede e os números das portas associadas com esta cópia da solicitação. Estas APIs são diferentes para cada vendedor de servidor da web seguro.

Assim, o módulo de plug-in 230 faz chamadas de API para o servidor da web 205 para obter o endereço de rede e o número de porta associado com o pacote da rede.

[0022] O módulo plug-in 230 abre então um soquete de comunicação da rede 260 entre o módulo plug-in 230 e o monitor 210 e, através de um pipe, passa o pacote descriptografado da rede de HTTPS, o endereço de rede e o número de porta para o monitor 210, na etapa 430. O monitor 210 executa então uma fusão e normalização. Baseado no endereço de rede e no número da porta, o monitor 210 primeiro executa a busca das estruturas de dados 240 em memória e tenta encontrar uma entrada que corresponde ao pacote da rede de HTTPS descriptografado passado, com base em seu endereço de rede e número de porta.

[0023] Se tal entrada for encontrada, o conteúdo criptografado armazenado do pacote da rede é substituído pelo conteúdo descriptografado recebido do módulo plug-in 230. Se uma correspondência não puder ser encontrada, o monitor 210 descarta os dados recebidos do módulo plug-in 230 e continua. Se uma entrada correspondente existir, uma solicitação de HTTPS de rede criptografada capturada, que normalmente não pode ser relacionada a um nome de URL, está agora pareado com um nome do URL e outros dados previamente criptografados, que dão os dados de volta aos monitores de rede que foram escondidos pelo protocolo de HTTPS. Assim, o monitor 210 tem, na estrutura de dados 240 em memória, toda a informação que normalmente teria se o protocolo de HTTP fosse não seguro, tal como um nome do URL de um recurso alvo

que pode ser uma imagem, um arquivo de programa, uma página de HTML, Java applet, etc.

[0024] Consequentemente, neste momento o monitor 210 pode extrair o nome do URL e outros dados do pacote de rede descriptografado armazenado e pode empregá-lo para várias soluções de gerenciamento de dados nas transações da rede, para serviços bancários e os outros serviços de software, aplicações e programas de tratamento de dados, incluindo a exploração de dados, reconhecimento de padrão, análise de dados, transcodificação de HTML para protocolo de aplicação sem fio (WAP - *Wireless applicatlon protocol*), conversão de dados, desempenho de monitoramento de aplicativos de servidor de HTTP da Internet e transferência de dados através de uma rede de comunicações entre um cliente e um local do usuário.

[0025] A presente invenção pode ser realizada em hardware, firmware ou software, ou qualquer combinação de hardware, firmware e software, ou em qualquer outro processo capaz de fornecer a funcionalidade divulgada. A implementação do método e do sistema da presente invenção pode ser realizada em uma forma centralizada em um sistema computadorizado de servidor, ou em uma forma distribuída onde os diferentes elementos estão espalhados através de diversos sistemas computadorizados interconectados. Qualquer tipo do sistema computadorizado ou do aparelho adaptado para realizar os métodos descritos aqui é adequado para executar as funções descritas aqui. A figura 1 ilustra um sistema computadorizado de uso geral com um grupo de programas de computador que, ao ser carregado e ao executar, controlam o

sistema computadorizado de tal maneira que realizam os aspectos do método da presente invenção. Os programas de computador podem ser embarcados em uma mídia utilizável por computador que compreendam todas as características que permitem a execução dos métodos descritos aqui e que podem realizar estes métodos quando carregados em um sistema computadorizado. No ambiente exemplificativo da figura 1, um sistema computadorizado do local de servidor 200 é compreendido por um ou mais processadores, não mostrados, que podem ser conectados a um ou mais dispositivos de armazenamento eletrônico, não mostrados, tais como unidades de disco.

[0026] A descrição antecedente das concretizações preferidas da invenção foi apresentada para os propósitos de ilustração e de descrição. Não se pretende ser exaustiva ou limitar a invenção à forma precisa divulgada. Muitas modificações e variações são possíveis à luz aos ensinamentos acima. Pretende-se que o escopo da invenção esteja limitado não por esta descrição detalhada, mas, ao invés disso, pelas reivindicações anexas.

REIVINDICAÇÕES

1. Método para mapear um pacote de solicitação de rede criptografado para sua cópia descriptografada em um servidor da web seguro da rede de computador **caracterizado pelo** fato de que compreende:

(a) criar (400) um módulo plug-in em um servidor da web seguro;

(b) salvar (410) pelo menos um endereço de rede e o número de porta a partir de um pacote de solicitação de rede criptografado capturado;

(c) obter (420) uma cópia descriptografada do pacote de solicitação de rede a partir do módulo de descriptografia dentro do servidor da web seguro pelo módulo plug-in; e

(d) obter (430) do módulo plug-in o pacote de rede descriptografado, o endereço de rede e o número de porta e mapeá-los no servidor web seguro para o pelo menos um endereço de rede e número de porta salvo.

2. Método, de acordo com a reivindicação 1, **caracterizado pelo** fato de que a etapa (d) ainda compreende a etapa de salvar o endereço de rede e o número de porta e o pacote de rede descriptografado em uma estrutura de dados (240) indexada pelo endereço de rede e pelo número de porta.

3. Método, de acordo com a reivindicação 1, **caracterizado pelo** fato de que a rede é a Internet, a criptografia é executada de acordo com o protocolo de transferência de hipertexto seguro (HTTPS) e a solicitação de rede criptografada é condescendente com a linguagem de marcação de hipertexto (HTML).

4. Método, de acordo com a reivindicação 1, **caracterizado pelo** fato de que os dados criptografados compreendem um nome de localizador de recurso universal (URL), um conteúdo específico de aplicação ou um link de hipertexto para um recurso remoto alvo que é escolhido do grupo que compreende texto, áudio, vídeo, gráfico, animação, imagem estática, arquivo de programa, página de HTML e Java applet.

5. Método, de acordo com a reivindicação 1, **caracterizado pelo** fato de que a descriptografia é executada pelo software de descriptografia do servidor da web convencional como parte do processamento normal do servidor da web, o módulo plug-in é escolhido do grupo que compreende o filtro da web e o NSAPI, e o endereço de rede e o número de porta do pacote de solicitação de rede criptografado capturado, são transferidos não criptografados.

6. Método, de acordo com a reivindicação 1, **caracterizado pelo** fato de que a etapa (c) compreende ainda a etapa em que o módulo plug-in invoca interfaces de programa de aplicação (APIs) no servidor da web seguro para obter o endereço de rede e o número de porta da solicitação criptografada original associada com o pacote de solicitação de rede descriptografado.

7. Método, de acordo com a reivindicação 1, **caracterizado pelo** fato de que a etapa (c) compreende ainda a etapa em que o módulo plug-in cria um soquete da rede e transfere o pacote da rede de HTTPS descriptografado, o endereço de rede e o número de porta através de um pipe.

8. Sistema para mapear um pacote de solicitação de rede criptografado para sua cópia descriptografada em um servidor da web seguro da rede de computador **caracterizado pelo** fato de que compreende meios para:

(a) criar (400) um módulo plug-in em um servidor da web seguro;

(b) salvar (410) pelo menos um endereço de rede e o número de porta a partir de um pacote de solicitação de rede criptografado capturado;

(c) obter (420) uma cópia descriptografada do pacote de solicitação de rede a partir do módulo de descriptografia do servidor da web seguro pelo módulo plug-in; e

(d) obter (430) do módulo plug-in o pacote de rede descriptografado, o endereço de rede e o número de porta e mapeá-los no servidor da web seguro pelo módulo de plug-in.

9. Sistema, de acordo com a reivindicação 8, **caracterizado pe**lo fato de que os meios para a etapa (d) ainda compreendem meios para salvar o endereço de rede e o número de porta e o pacote de rede descriptografado em uma estrutura de dados (240) indexada pelo endereço de rede e pelo número de porta.

10. Sistema, de acordo com a reivindicação 8, **caracterizado pelo** fato de que a rede é a Internet, a criptografia é executada de acordo com o protocolo de transferência de hipertexto seguro (HTTPS) e a solicitação de rede criptografada é condescendente com a linguagem de marcação de hipertexto (HTML).

11. Sistema, de acordo com a reivindicação 8, **caracterizado pelo** fato de que os dados criptografados

compreendem um nome de localizador de recurso universal (URL), um conteúdo específico de aplicação ou uma ligação de hipertexto a um recurso remoto alvo que é escolhido do grupo que compreende texto, áudio, vídeo, gráfico, animação, imagem estática, arquivo de programa, página de HTML e Java applet.

12. Sistema, de acordo com a reivindicação 8, **caracterizado pelo** fato de que a descriptografia é executada pelo software da descriptografia do servidor da web convencional como parte do processamento normal do servidor da web, o módulo plug-in é escolhido do grupo que compreende o filtro da web e o NSAPI, e o endereço de rede e o número de porta do pacote de solicitação de rede criptografado capturado, são transferidos não criptografados.

13. Sistema, de acordo com a reivindicação 8, **caracterizado pelo** fato de que os meios para a etapa (c) compreendem ainda meios em que o módulo plug-in invoca interfaces de programa de aplicação (APIs) no servidor da web seguro para obter o endereço de rede e o número de porta da solicitação criptografada original associada com o pacote de solicitação da rede descriptografado.

14. Sistema, de acordo com a reivindicação 8, **caracterizado pelo** fato de que os meios para a etapa (d) compreendem ainda meios em que o módulo plug-in cria um soquete de rede e transfere o pacote da rede de HTTPS descriptografado, o endereço de rede e o número de porta através de um pipe.

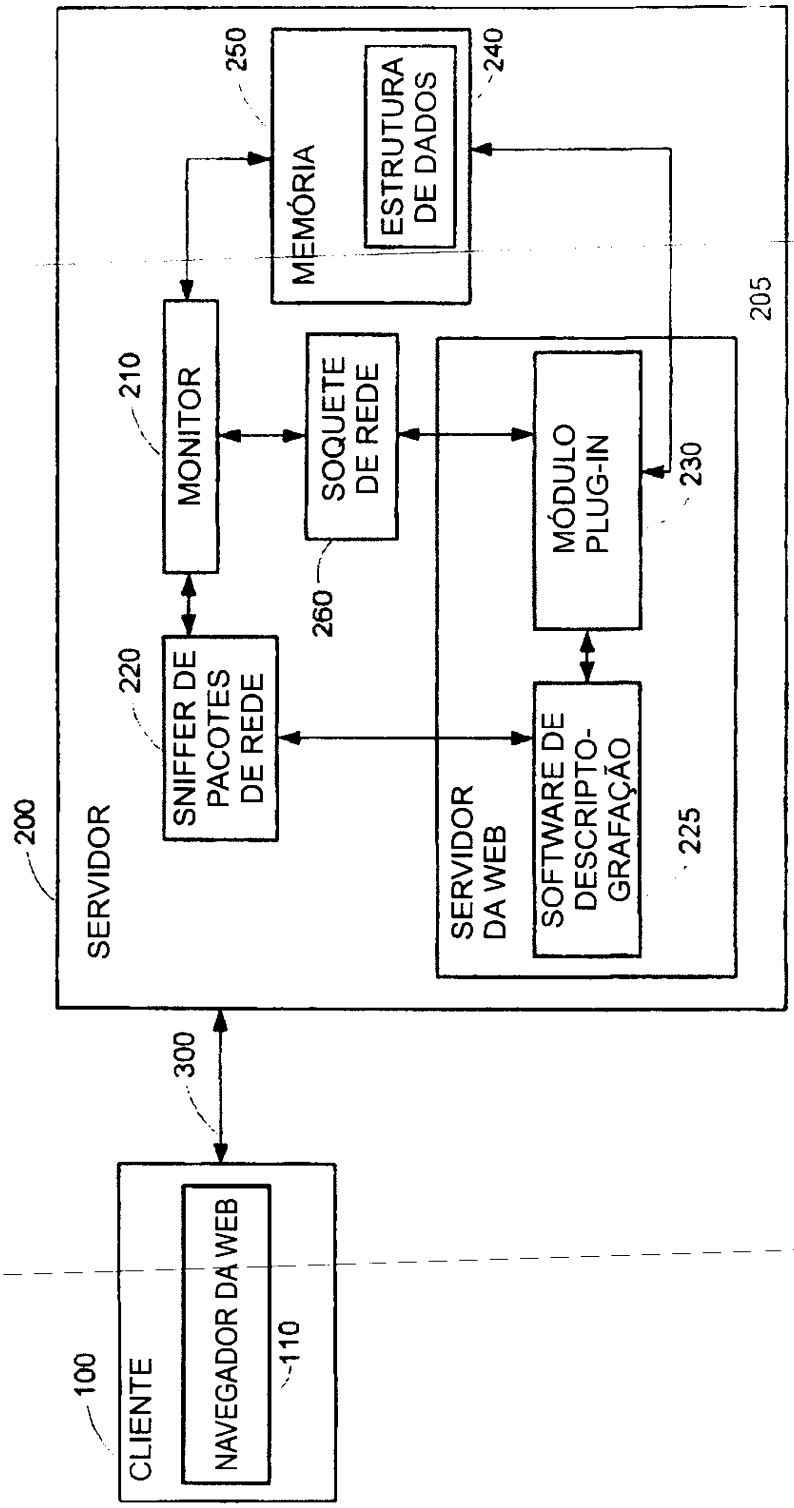
CLIENTE
100
NAVEGADOR DA WEB
110
300
SERVIDOR
200
SNIFFER DE PACOTES DE REDE
220
MONITOR
210
SOQUETE DE REDE
260
MEMÓRIA
250
ESTRUTURA DE DADOS
240
205
SERVIDOR DA WEB
225
SOFTWARE DE DESCRIPTO-GRAFAÇÃO
MÓDULO PLUG-IN
230

Figura 1

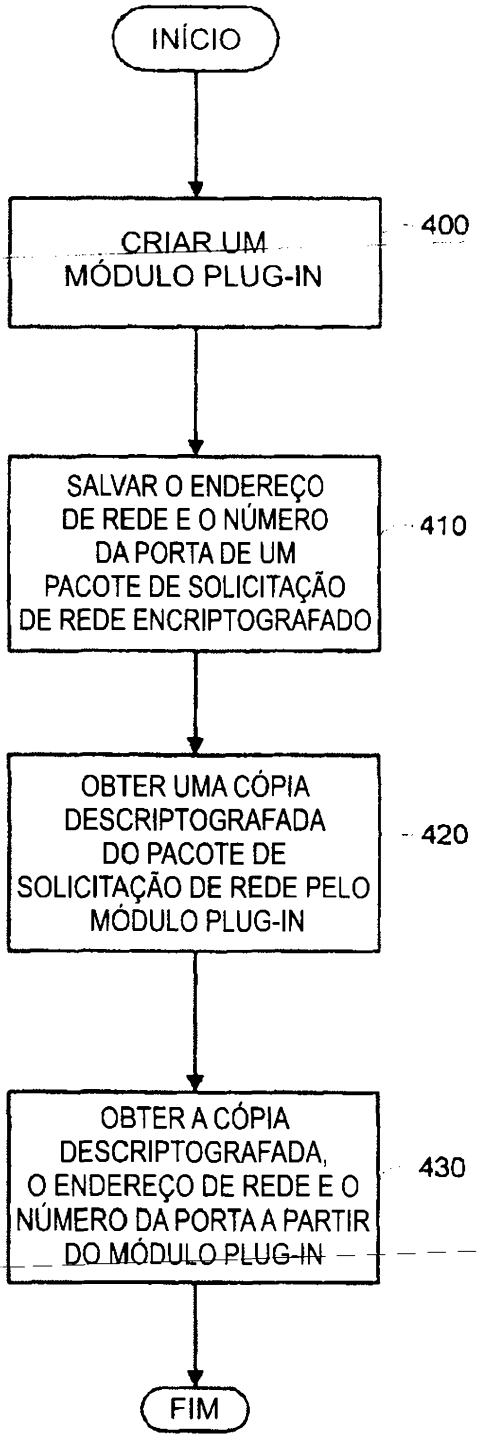
INÍCIO
CRIAR UM MÓDULO PLUG-IN
400
SALVAR O ENDEREÇO DE REDE E O NÚMERO DA PORTA DE UM PACOTE DE SOLICITAÇÃO DE REDE ENCRIPTOGRAFADO
410
OBTER UMA CÓPIA DESCRIPTOGRAFADA DO PACOTE DE SOLICITAÇÃO DE REDE PELO MÓDULO PLUG-IN
420
OBTER A CÓPIA DESCRIPTOGRAFADA, O ENDEREÇO DE REDE E O NÚMERO DA PORTA A PARTIR DO MÓDULO PLUG-IN
430
FIM

Figura 2