República Federativa do Brasil
Ministério do Desenvolvimento, Indústria e do Comércio Exterior
Instituto Nacional da Propriedade Industrial.

(21) **PI0610539-4 A2**

BRPI0610539A2

(22) Data de Depósito: 27/03/2006
(43) Data da Publicação: 29/06/2010
(RPI 2060)

(51) Int.Cl.:
G06Q 20/00
G06F 21/00

(54) Título: **SISTEMA DE SEGURANÇA DE REDE**

(30) Prioridade Unionista: 21/04/2005 GB 05080445

(73) Titular(es): PALM TREE TECHNOLOGY IP LIMITED

(72) Inventor(es): DELON DOTSON, MARC LOY

(74) Procurador(es): Claudia Christina Schulz

(86) Pedido Internacional: PCT EP2006003072 de 27/03/2006

(87) Publicação Internacional: WO 2006/111270de 26/10/2006

(57) Resumo: A presente invenção refere-se a um método de autenticação de uma transação entre um dispositivo local, sob controle de um usuário, e um servidor remoto, compreendendo: - determinar uma série de dados específicos ao dispositivo local; - determinar uma série de dados específicos para o usuário do dispositivo; - transmitir a série de dados específicos de dispositivo e a série de dados específicos de usuário para uma máquina de criptografia remota; e - gerar na máquina de criptografia remota uma série de modelos de dados de uso único, cada modelo compreendendo itens selecionados aleatoriamente da série de dados específicos de dispositivo e da série de dados específicos de usuário; o método compreendendo ainda, durante autenticação: - enviar um modelo de dados da máquina para o dispositivo local; - usar o modelo de dados para interrogar o dispositivo local para os itens de dados específicos de dispositivo; - usar o modelo de dados para interrogar o usuário, para proporcionar os itens de dados específicos de dispositivo no modelo; e - comparar os itens de dados proporcionados pelo dispositivo local e o usuário, em resposta à interrogação aos itens de dados usados para criar o modelo para autenticar a transação.

SISTEMA DE SEGURANÇA DE REDE

CAMPO DA INVENÇÃO

A presente invenção se refere a sistemas de segurança para operação com dispositivos ligados em rede. Em particular, a invenção proporciona métodos e sistemas para garantir a identidade de um usuário em um ambiente de transação ligado em rede.

FUNDAMENTOS DA INVENÇÃO

Um ambiente, no qual essa invenção encontra aplicação particular, é aquele de transações seguras pela Internet. No entanto, como vai ser evidente, a invenção não é limitada a esses usos e pode ser aplicada a transações entre os dispositivos, usando vários meios de comunicação.

Vários métodos foram desenvolvidos para proporcionar segurança em transações pela Internet. Um desses exemplos é o de Camadas de Soquetes Seguros (SSL), desenvolvidas pela Netscape como um protocolo de segurança para transações únicas. Essas podem ser usadas para eventos únicos, tal como pagamento de cartão de crédito para uma compra feita por um lugar na Internet. No entanto, a maior parte das transações não são de evento único e um outro nível de segurança é necessário. A mais comum dessas é o uso de códigos de acesso, números de pinos ou senhas. Esses impõem que um usuário introduza um código "secreto" para confirmar

a identidade do usuário e criar um canal de comunicação segura entre o usuário e o provedor de serviço, tal como o banco. Desde que o código se mantenha secreto, a comunicação pode ser segura. No entanto, pode ser relativamente fácil determinar o código secreto, ou por interrogação do computador no qual o código é salvo, registrando as batidas no teclado, quando o código é introduzido, observando a entrada de código ou um registro escrito do código, ou por simples tentativa e erro, com base em análise matemática. Alguns sistemas tentam aperfeiçoar o nível de segurança por combinações de códigos e questões selecionadas, que se referem às informações pessoais do usuário. No entanto, esses ainda estão submetidos às mesmas deficiências gerais.

Um nível de segurança aperfeiçoado pode ser obtido por uso de um cartão inteligente (um cartão conduzindo um circuito integrado IC). O processamento limitado no circuito integrado do cartão propicia o uso de uma criptografia mais complexa. Também, proporciona uma chave física que deve estar presente juntamente com o código relevante. Há considerações práticas que fazem com que o uso desses cartões não seja muito desejável. O computador do usuário deve ser capaz de ler o cartão, os cartões são relativamente caros e os cartões precisam de maneira segura para emissão e distribui.

~~Todos esses sistemas se baseiam apenas em informações~~ do usuário. Essa invenção faz uso de informações

específicas de dispositivo, para aperfeiçoar o nível de segurança.

DESCRIÇÃO DA INVENÇÃO

Um aspecto da invenção compreende um método de autenticação de uma transação entre um dispositivo local, sob controle de um usuário, e um servidor remoto, compreendendo:

- determinar uma série de dados específicos ao dispositivo local;

- determinar uma série de dados específicos para o usuário do dispositivo;

- transmitir a série de dados específicos de dispositivo e a série de dados específicos de usuário para uma máquina de criptografia remota; e

- gerar na máquina de criptografia remota uma série de modelos de dados de uso único, cada modelo compreendendo itens selecionados aleatoriamente da série de dados específicos de dispositivo e da série de dados específicos de usuário;

o método compreendendo ainda, durante autenticação:

- enviar um modelo de dados da máquina para o dispositivo local;

- usar o modelo de dados para interrogar o dispositivo local para os itens de dados específicos de dispositivo;

- usar o modelo de dados para interrogar o usuário, para proporcionar os itens de dados específicos de dispositivo no modelo; e

- comparar os itens de dados proporcionados pelo dispositivo local e o usuário, em resposta à interrogação aos itens de dados usados para criar o modelo para autenticar a transação.

De preferência, o método inclui a etapa de carregar um agente de software no dispositivo local, o agente de software manipulando a determinação dos dados específicos de dispositivo, proporcionando uma interface para o usuário introduzir os dados específicos de usuário, e a de comunicar esses dados, em forma criptografada, à máquina de criptografia.

Prefere-se também que, após o uso do modelo de dados em uma operação de autenticação, que o modelo seja deletado da série.

Em uma concretização da invenção, o modelo de dados é enviado para o dispositivo local, imediatamente antes da transação, para que seja autenticado, e a resposta é enviada do dispositivo local para o servidor remoto, após recebimento e antes da transação ocorrer.

O dispositivo local pode ser um computador, um telefone móvel, um PDA ou qualquer outro desses dispositivos. O dispositivo local pode conectar-se ao servidor remoto por um canal de comunicações adequado, tal como a Internet, conexão sem fio, GPRS, WAN, LAN, etc.

Os dados específicos para o dispositivo local podem compreender os dados relativos à configuração física do dispositivo, tais como os números id (identificadores) para os componentes, tais como os discos rígidos, CPUs, etc., e configuração de software e firmware, tais como tipo e versão de OS, versão de BIOS, etc.

Os dados específicos para o usuário compreendem tipicamente informações conhecidas do usuário e proporcionadas em resposta.

MODO(S) PARA CONDUÇÃO DA INVENÇÃO

O aspecto da invenção apresentado a seguir é descrito em relação a um computador como um dispositivo local. Vai ser evidente que a mesma tecnologia pode ser aplicada a

muitos diferentes tipos de dispositivos, tais como telefones fixos, telefones móveis, PDAs, etc.

Cada computador tem determinadas propriedades que são únicas àquela máquina. Incluem números de identificação ou números de registro da CPU, placa-mãe ou discos rígidos, por exemplo. Outras informações contidas dentro da máquina podem incluir tamanho do disco rígido, capacidade de armazenamento da RAM, data de compra ou registro, versão de BIOS, sistema operacional, nome da máquina, etc. Esses dados são tipicamente armazenados no disco rígido da máquina (ou equivalente). Ainda que poucos desses itens de dados sejam absolutamente únicos, exceto possivelmente os números de identificação ou registro, há itens de dados diferentes suficientes entre esses elementos em computadores aparentemente idênticos, que a probabilidade de qualquer computador ter dados idênticos é muito baixa. No entanto, por conta deles mesmos, esses dados não são absolutamente seguros. Se um computador for conectado a uma rede, é relativamente direto interrogar a máquina, para proporcionar esses dados e imitar essa máquina.

Para evitar esse problema, a presente invenção também usa dados específicos de usuário. Essas são informações proporcionadas pelo usuário e de conhecimento apenas dele. Essas informações podem compreender informações, tais como data de nascimento, nome de solteira da mãe, etc. No entanto, uma vez que essas informações também podem ser obtidas de outras fontes, prefere-se que os dados

específicos de usuário também incluam as informações relativas às preferências pessoais, tais como cor favorita, ou informações pessoais incomuns tais como nome do animal de estimação ou assemelhados. Proporcionando-se itens suficientes dessas informações, a probabilidade de outro usuário ter as mesmas informações pessoais é muito baixa.

Esses dois conjuntos de dados formam a base da invenção. O objeto é proporcionar um sistema que requer informações selecionadas aleatoriamente de ambos os conjuntos, para autenticar a transação.

A invenção se refere à transação entre os dispositivos locais e os servidores remotos. Os exemplos típicos dessas transações são o sistema bancário via Internet e as centrais de vendas pela Internet. Nessas transações, um usuário usa o dispositivo local para comunicar-se com o servidor remoto, para pedir informações ou instruir ações (por exemplo, ver extratos bancários, instruir compras ou transferências, etc.). Em virtude do valor da transação, qualquer que seja em termos de informações pessoais (nomes, endereços, números de conta, extratos bancários, etc.) ou de valor comercial direto (pagamentos, etc.), é desejável que ambos o usuário e o provedor de serviço autentiquem a transação para confirmar que o usuário está habilitado a submeter ou receber as informações ou instruir a ação. A abordagem básica para essa autenticação, tanto na técnica anterior quanto na presente invenção, é que o servidor

remoto interroga o usuário pelo dispositivo local, para dados que confirmem a identidade.

Na presente invenção, a maneira na qual os dois conjuntos de dados são usados é por uso de uma máquina de criptografia. Em uma transação típica, isso vai ser de responsabilidade da entidade que controla o servidor remoto. No entanto, em muitos casos, a máquina de criptografia vai ficar em um servidor separado e vai agir em resposta aos pedidos do servidor remoto.

Para configurar o dispositivo local, um agente de software é instalado nele. Esses agentes de software são comumente usados para várias aplicações de softwares. O agente de software pode ser carregado por uma conexão em rede, um CD ou qualquer outra abordagem. Uma vez instalado, o agente de software interroga o servidor remoto para obter os dados específicos de dispositivo. Os tipos de dados vão ser predeterminados no agente e podem incluir aqueles dados específicos de dispositivo indicados acima. A abordagem desejada é que essa interrogação e a seleção de dados sejam automáticas. É possível que isso possa ser também feito manualmente por uso de caixas de diálogo e campos de introdução de dados. Os dados específicos de usuário vão ser coletados por uso de caixas de diálogo e campos de introdução de dados, os dados sendo introduzidos em resposta às perguntas apresentadas pelo agente de software. Ainda que perguntas predefinidas sejam preferidas,

considera-se também que o usuário pode também introduzir as suas próprias perguntas e respostas.

Os dados coletados pelo agente de software são transmitidos para a máquina de criptografia, por uma conexão em rede, tipicamente em forma criptografada. A máquina de criptografia então mistura ou "munges" (mung = triturar ate reduzir a nada) os dois conjuntos de dados e cria uma série de modelos de dados de uso único, que são eles próprios armazenados em forma criptografada. Há várias técnicas e algoritmos conhecidos para triturar os dados que podem ser usados. Em tudo isso, o que é importante é que após trituração, os dados não são reconhecidos como os seus dados-fonte originais.

Cada modelo de dados compreende uma combinação selecionada aleatoriamente de itens de dados de cada conjunto: específicos de usuário e específicos de dispositivo. Vários desses modelos podem ser preparados de antemão, por exemplo, 500 modelos armazenados prontos para uso. É também possível criar cada modelo apenas quando necessário, com nenhum sendo armazenado. No entanto, isso pode retardar o processo inaceitavelmente.

Cada modelo de dados é intencionado para ser usado apenas uma vez. Nesse aspecto, o conjunto de modelos de dados são similares aos caracteres de uso único usados para chaves de códigos.

Em uso, o usuário inicia uma transação com o servidor a partir do dispositivo local. Quando a autenticação é necessária, a aplicação de software de autenticação, no servidor remoto, pede que o modelo seja emitido pela máquina de criptografia. Ou o modelo seguinte no conjunto é emitido ou um novo modelo é gerado pela máquina. O modelo é enviado para o servidor e para o dispositivo local. A aplicação de software no servidor remoto determina, a partir dos dados proporcionados pelo agente de software no dispositivo local, os itens de dados específicos para autenticar a transação do modelo. O agente de software no dispositivo local interroga o dispositivo para os dados específicos de dispositivo e exibe caixas de diálogo e campos de introdução de dados para os dados específicos de usuário. Uma vez que esses dados são introduzidos, eles são enviados, em forma criptografada, para o servidor remoto, no qual a aplicação de software compara os dados proporcionados do dispositivo local com os dados derivados da máquina como corretos, para comparação com aquele modelo de dados. Se os itens de dados estão corretos, a transação pode ser autenticada. Se não, a transação pode ser negada.

O método da presente invenção tem várias vantagens. Essas incluem o fato de que a interceptação dos dados transmitidos do dispositivo local para o servidor não é de uso posterior, uma vez que outro modelo vai requerer uma combinação diferente de itens de dados. Também, a alteração de um parâmetro de dispositivo, tal como uma unidade de disco, pode ser acomodada por novo registro dos dados

específicos de dispositivo, tal como um evento, e geração de novos modelos.

As aplicações típicas compreendem transação bancárias em linha e comercialização pela Internet. No entanto, um uso particular desse método pode ser na distribuição de música pela Internet. Nesse caso, o arquivo de música digital é transmitido para o dispositivo local, seguinte à autenticação, como descrito acima. Os dados específicos de dispositivo são mantidos com o arquivo digital e o reprodutor configurado de modo que apenas toque se o dispositivo no qual o arquivo vai ser reproduzido puder proporcionar os dados necessários para aqueles no arquivo. Desse modo, o arquivo de música só pode ser reproduzido no dispositivo para o qual tenha sido transmitido originalmente. Isso permite que os detentores dos direitos das músicas impeçam a distribuição não autorizada de cópias do arquivo de música, uma vez que não vão ser reprodutíveis em qualquer outro dispositivo.

Considera-se que os métodos de acordo com a invenção são de ampla aplicação e não são limitados a qualquer uma forma particular de dispositivo ou transação. A implementação em software dos conceitos é direta.

REIVINDICAÇÕES

1. Método de autenticação de uma transação entre um dispositivo local, sob controle de um usuário, e um servidor remoto, caracterizado pelo fato de que compreende:

- determinar uma série de dados específicos ao dispositivo local;
- determinar uma série de dados específicos para o usuário do dispositivo;
- transmitir a série de dados específicos de dispositivo e a série de dados específicos de usuário para uma máquina de criptografia remota; e
- gerar na máquina de criptografia remota uma série de modelos de dados de uso único, cada modelo compreendendo itens selecionados aleatoriamente da série de dados específicos de dispositivo e da série de dados específicos de usuário;

o método compreendendo ainda, durante autenticação:

- enviar um modelo de dados da máquina para o dispositivo local;
- usar o modelo de dados para interrogar o dispositivo local para os itens de dados específicos de dispositivo;
- usar o modelo de dados para interrogar o usuário, para proporcionar os itens de dados específicos de ~~dispositivo no modelo; e~~

- comparar os itens de dados proporcionados pelo dispositivo local e o usuário, em resposta à interrogação aos itens de dados usados para criar o modelo para autenticar a transação.

2. Método de acordo com a reivindicação 1, caracterizado pelo fato de que os dados específicos de usuário e os dados específicos de dispositivo são reunidos por meio de um agente de software, instalado no dispositivo.

3. Método de acordo com a reivindicação 1 ou 2, caracterizado pelo fato de que a máquina de criptografia gera a série de modelos, que é armazenada antes de uso.

4. Método de acordo com a reivindicação 1 ou 2, caracterizado pelo fato de que a máquina de criptografia gera cada modelo em resposta a um pedido para autenticação do servidor remoto.

5. Método de acordo com qualquer uma das reivindicações 1 a 4, caracterizado pelo fato de que a transação compreende o envio de um arquivo executável do servidor para o dispositivo, o método incluindo ainda associar os dados específicos de dispositivo com o arquivo executável, de modo que só possam ser executados naquele dispositivo.

6. Método de acordo com qualquer uma das reivindicações 1 a 5, caracterizado pelo fato de que a transação compreende proporcionar informações, compra em linha ou transferência de música.

RESUMO

SISTEMA DE SEGURANÇA DE REDE

A presente invenção refere-se a um método de autenticação de uma transação entre um dispositivo local, sob controle de um usuário, e um servidor remoto, compreendendo: - determinar uma série de dados específicos ao dispositivo local; - determinar uma série de dados específicos para o usuário do dispositivo; - transmitir a série de dados específicos de dispositivo e a série de dados específicos de usuário para uma máquina de criptografia remota; e - gerar na máquina de criptografia remota uma série de modelos de dados de uso único, cada modelo compreendendo itens selecionados aleatoriamente da série de dados específicos de dispositivo e da série de dados específicos de usuário; o método compreendendo ainda, durante autenticação: - enviar um modelo de dados da máquina para o dispositivo local; - usar o modelo de dados para interrogar o dispositivo local para os itens de dados específicos de dispositivo; - usar o modelo de dados para interrogar o usuário, para proporcionar os itens de dados específicos de dispositivo no modelo; e - comparar os itens de dados proporcionados pelo dispositivo local e o usuário, em resposta à interrogação aos itens de dados usados para criar o modelo para autenticar a transação.