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

(21) **PI0806772-4 A2**

BRPI0806772A2

(22) Data de Depósito: 15/01/2008
(43) Data da Publicação: 13/09/2011
(RPI 2123)

(51) Int.Cl.:
H04L 29/10
H04L 12/14
H04Q 7/22
G06Q 10/00

(54) Título: MÓDULO DE SEGURANÇA TENDO UM AGENTE SECUNDÁRIO EM COORDENAÇÃO COM AGENTE HOST

(30) Prioridade Unionista: 16/01/2007 US 60/880,800

(73) Titular(es): Absolute Software Corporation

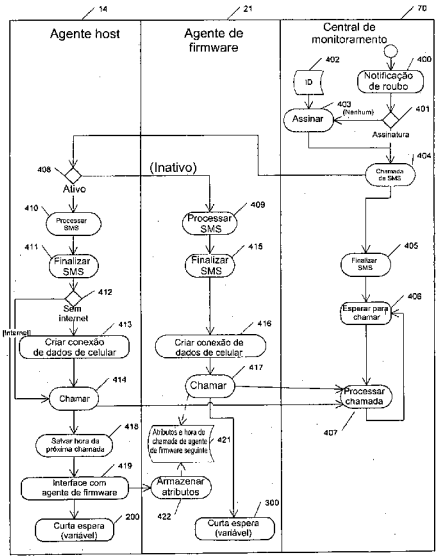
(72) Inventor(es): William Doyle Gordon

(74) Procurador(es): Dannemann ,Siemsen, Bigler & Ipanema Moreira

(86) Pedido Internacional: PCT IB2008000753 de 15/01/2008

(87) Publicação Internacional: WO 2008/090470de 31/07/2008

(57) Resumo: MÓDULO DE SEGURANÇA TENDO UM AGENTE SECUNDÁRIO EM COORDENAÇÃO COM UM AGENTE HOST. A presente invenção refere-se a um módulo de segurança implantado em um dispositivo host, que provê um agente secundário que opera em coordenação com o agente host no dispositivo host, mas opera independente do sistema operacional de host do dispositivo host de modo a acessar independentemente uma interface de rede de comunicação existente no dis- positivo host ou uma interface de rede dedicada separada, quando disponível. Em um aspecto, a presente invenção habilita serviços robustos de rastreamento de bens e recuperação de roubo. O sistema compreende uma central de monitoramento; um ou mais dispositivos monitorados; um módulo de segurança nos dispositivos monitorados; e uma ou mais redes de comunicação ativa. Os dispositivos monitorados podem ser dispositivos independentes, tais como computadores (por exemplo, computadores portáteis ou de mesa), ou um dispositivo ou um subsistema incluído em um sistema. Um dispositivo monitorado compreende um módulo de segurança, um agente host e um software para suportar o agente host executado no OS do dispositivo monitorado.



Relatório Descritivo da Patente de Invenção para **"MÓDULO DE SEGURANÇA TENDO UM AGENTE SECUNDÁRIO EM COORDENAÇÃO COM UM AGENTE HOST".**

O presente pedido reivindica a prioridade do Pedido de Patente Provisório U.S. Nº 60/880 800, depositado em 16 de janeiro de 2007. Esse documento e outras publicações aqui mencionados são incorporados em sua totalidade ao presente documento à guisa de referência, como se plenamente aqui apresentados.

ANTECDENTES DA INVENÇÃO

1. Campo da Invenção

A presente invenção refere-se a um módulo de segurança para dispositivos (por exemplo, dispositivos eletrônicos), nomeadamente, um módulo de segurança para comunicação com um local externo para o monitoramento remoto dos dispositivos com o propósito, por exemplo, de rastrear bens e ajudar na recuperação de bens roubados ou perdidos, e, mais particularmente, a um módulo de segurança sem fio para tais fins. Esses dispositivos podem incluir, sem limitações, dispositivos controlados por processador, tais como computadores, e sistemas que incluem dispositivos baseados em processador, tais como fotocopiadoras.

2. Descrição da Técnica Relacionada

A Patente U.S. Nº 4 818 998 cedida à Lo-Jack Corporation descreve um método para a recuperação de roubo de automóveis, cujos veículos rastreados pela polícia recebem transmissões periódicas de rádio do tipo transponder automaticamente ativadas por sinais de ativação de comando transmitidos na mesma frequência da portadora com informações de identificação de veículo codificadas que fazem com que o transponder do veículo em questão responda.

A tecnologia OnStar da GM provê uma plataforma genérica sem fio para a liberação de serviços a um sistema móvel. No caso da OnStar, o sistema móvel é um automóvel, e não um dispositivo portátil de usuário, como um computador portátil. O OnStar pode ser usado para a recuperação de roubo e pode ser utilizado para fornecer também outros serviços. Com o

OnStar, um dispositivo contata uma estação remota após um evento iniciado por um usuário.

A Patente U.S. Nº 5 748 084 refere-se a um sistema de rastreamento, comunicação e gerenciamento para um computador portátil ou dispositivo similar, onde um radiofarol ou transceptor do computador implementa etapas de integridade de arquivo ou de recuperação de dispositivo, tais como a transmissão, a destruição ou a codificação de dados sensíveis, e que emitem um sinal RF rastreável. Uma combinação de hardware e software dentro do radiofarol ou do sistema do host inicia e coordena a operação de recursos de comunicação e de segurança. Por exemplo, a comunicação poderá ser iniciada ao não se conseguir entrar uma senha correta, no caso de um evento de violação ou por meio de um sinal transmitido para o dispositivo. Sob circunstâncias normais, o radiofarol implementa uma função de comunicação-padrão com o dispositivo, tal como um e-mail, uma mensagem de voz ou um fax. Uma lógica de detecção de violação é implementada no software ou no hardware. Uma chamada de dados recebida de preferência contém comandos de controle de radiofarol de baixo nível que são interpretados pelo radiofarol antes do alerta ou da passagem dos dados para o computador. De preferência, os códigos de baixo nível operam no nível do sistema BIOS para a realização de funções de emergência quando componentes de plug-ins ou de software de níveis mais altos são ignorados ou removidos.

A Patente U.S. Nº 6 362 736 provê um sistema para localizar automaticamente um objeto eletrônico pessoal. O sistema inclui pelo menos dois comunicadores sem fio. Quando a segurança do sistema é comprometida, conforme determinado por um sensor de violação ou por um usuário que toma conhecimento de um roubo, e o acesso a uma rede de computador ou de uma rede sem fio se encontra disponível, a localização, conforme determinada por um aparelho GPS é transmitida através de um comunicador.

A Patente U.S. Nº 6 636 175 descreve uma invenção que permite a um usuário localizar um dispositivo de paginação remoto situado em uma pessoa ou em uma propriedade de modo a determinar a sua posição

física. A posição do dispositivo remoto é determinada por um transceptor GPS e é enviada para um provedor de serviços de posição. A posição do dispositivo remoto é então exibida em um mapa para o usuário. Em uma modalidade, uma rede de comunicação Bluetooth é utilizada, por exemplo, em um parque de diversões ou em um shopping center nos quais hubs Bluetooth podem ser configurados a intervalos regulares.

A Patente U.S. Nº 6 950 946 descreve um método para descobrir e, opcionalmente, recuperar sistemas de computador instaláveis em rede que foram roubados ou extraviados. Um sistema de computador anexável em rede gera informações de identidade que incluem um identificador ID seguro, protegido, que usa uma chave de criptografia. Estas informações de identidade são enviadas automaticamente através de uma interface de rede para um módulo servidor, onde as mesmas são utilizadas no sentido de determinar se o respectivo sistema de computador foi declarado perdido ou roubado. O esquema é de preferência implementado em um hardware, uma vez que um sistema operacional (OS) ou uma implementação de software poderá ser alternadamente modificada no sentido de desativar o esquema.

A Publicação do Pedido de Patente U.S. Nº 2003/0117316 descreve sistemas e métodos para localizar e rastrear um dispositivo sem fio, incluindo um banco de dados remoto para o armazenamento de informações de localização para o dispositivo sem fio. Os sistemas e métodos podem incluir e trabalhar em conjunto com um modo de segurança do dispositivo sem fio, que direciona o dispositivo sem fio a entrar um modo de uso de baixa potência, um modo de suspensão, ou um modo de desligamento durante períodos de inatividade. Um serviço de despertador eletrônico ou uma senha são, de preferência, necessários para desativar ou cancelar o modo de segurança.

A Publicação do Pedido de Patente U.S. Nº 2006/0123307 descreve um aparelho, sistemas e métodos de segurança de plataforma computacional. O aparelhos e os sistemas, bem como os métodos e os artigos, podem operar de modo a receber um estado a partir de um módulo independente do sistema OS, capaz de prover informações de localização geográfi-

ca independentes do sistema OS, associadas a um dispositivo, para uma rede em algum momento antes de executar o sistema operacional. O módulo independente do sistema OS pode ser anexado ao, localizado juntamente com, ou separado do dispositivo.

Os sistemas acima referidos compartilham pelo menos uma falha comum, ou seja, a incapacidade de se comunicar externamente, caso a interface de comunicação existente se torne indisponível ou não-funcional.

A Absolute Software Corporation, cessionária da presente invenção, desenvolveu e está comercializando o Computrace, um produto ou serviço, que rastreia bens com segurança e recupera bens perdidos ou roubados, e o AbsoluteTrack, uma solução para o rastreamento seguro de bens, e gerenciamento de inventários, acionado pela plataforma tecnológica do Computrace. O Computrace implanta um agente secreto, que é um software cliente que reside no disco rígido dos computadores principais. Uma vez instalado, o agente automaticamente contata a central de monitoramento, transmitindo regularmente informações de localização e de todos os pontos de dados dos bens descobertos por si só. Uma comunicação em curso entre o agente e a central de monitoramento não requer nenhuma intervenção por parte do usuário, e é mantida pela Internet ou através de uma ligação telefônica. Contanto que o computador esteja ligado e tenha uma conexão com uma linha telefônica ou acesso à Internet (através de um provedor ISP ou através de uma rede empresarial), o agente Computrace poderá relatar dados relativos a bens para a central de monitoramento. A comunicação livre de intervenção entre o agente e a central de monitoramento garante que o usuário autorizado do agente venha a ter acesso seguro a informações de localização atualizadas e a dados exaustivos dos bens de todo o inventário do seu computador. Quer seja usado independentemente ou como complemento a uma ferramenta de gerenciamento de bens existentes, o AbsoluteTrack tem sido um serviço de aplicação de boa relação custo – benefício, ajudando a empresas de todos os tamanhos a monitorar, remotamente, computadores móveis ou computadores de mesa, e executa diariamente as funções de rastreamento de inventários de hardware e software. O Compu-

trace tem sido um instrumento eficaz para rastrear o roubo de computadores portáteis, e recuperar computadores móveis roubados.

A tecnologia subjacente a diversos produtos e serviços Computrace tem sido divulgada e patenteada nos Estados Unidos e em outros países, cujas patentes têm sido cedidas comumente à Absolute Software Corporation. Vide, por exemplo, as Patentes U.S. Nºs 5 715 174, 5 764 892, 5 802 280, 6 244 758, 6 269 392, 6 300 863 e 6 507 914; e suas patentes estrangeiras relacionadas. Outras informações sobre o AbsoluteTrack têm sido publicadas pela Absolute Software Corporation (por exemplo, o "AbsoluteTrack - Secure Computer Asset Tracking Solution", um documento informal, publicado em 25 de abril de 2003).

Os modos de comunicação à disposição do agente traz um impacto direto à capacidade de rastrear o computador. Embora o agente Computrace possa atualmente se comunicar através de uma Ethernet, um WiFi, e de outras conexões de Internet ou telefone, seria desejável desenvolver um aparelho que permita ao agente se comunicar, caso estas conexões existentes estejam indisponíveis ou se tornem indisponíveis, por exemplo, devido ao não uso ou da não conexão do computador por um período de tempo prolongado. Seria desejável se iniciar comunicações em tempo real, em oposição a uma chamada programada. Também seria desejável se comunicar quando o agente Computrace é incapaz de se comunicar devido à ausência de um sistema OS de host, à presença de um sistema OS não suportado, à presença de um firewall ou de um sistema host não acionado. Seria também desejável poder despertar o sistema do host e executar medidas de proteção de dados ou outras operações de serviço. Um ou mais desses aspectos desejáveis são providos pelo sistema de rastreamento de bens e de recuperação de roubo descrito abaixo.

SUMÁRIO DA INVENÇÃO

A presente invenção refere-se a um módulo de segurança implantado em um dispositivo host (por exemplo, um dispositivo eletrônico), que provê um agente secundário que funciona em coordenação com o agente host no dispositivo host, mas opera independentemente do sistema ope-

racional de host do dispositivo host a fim de acessar independentemente a interface de rede de comunicação existente no dispositivo host ou uma interface de rede dedicada separada, se disponível. O módulo de segurança pode ser implantado em conjunto com serviços que podem incluir o rastreamento de bens, o gerenciamento de bens, a recuperação de bens, a exclusão de dados, a implantação de um software, etc.

Em um aspecto, a presente invenção habilita serviços robustos de recuperação de roubo e de rastreamento de bens. O sistema inclui uma central de monitoramento; um ou mais dispositivos monitorados; um módulo de segurança nos dispositivos monitorados; uma ou mais redes de comunicação ativa; uma assinatura, se necessário, para pelo menos uma rede de comunicação. Os dispositivos monitorados podem ser dispositivos independentes, tais como os computadores (por exemplo, os computadores portáteis ou de mesa), ou um dispositivo ou um subsistema incluído em um sistema. Um dispositivo monitorado compreende um módulo de segurança, agente host e um software a fim de suportar o agente host executado no sistema OS do dispositivo monitorado.

Em uma modalidade, o módulo de segurança inclui uma ou mais interfaces de rede ou o acesso compartilhado às interfaces do host; um processador específico que faz interface com a rede; um armazenamento persistente a partir do qual o ambiente operacional ou o sistema do módulo ou subsistema de segurança e os aplicativos que são executados no processador específico são carregados, um agente de firmware, secundário executado no ambiente ou sistema operacional em execução no processador específico; um armazenamento persistente para utilização pelo agente de firmware; zero ou mais tecnologias de determinação de localização, tais como o GPS. O módulo de segurança pode ter uma interface de rede que é dedicada a comunicações relativas à segurança. Uma ou mais interfaces de rede podem ter uma interface de rede WWAN. O módulo de segurança inclui um hardware ou um software de interface opcional que permite que o módulo de segurança inicie ou continue o sistema OS do host. O módulo de segurança pode ou não ter o sua própria fonte de alimentação.

O módulo ou subsistema de segurança pode ou não prover as funções normais de um modem de dados celulares, incluindo (1) a capacidade de o computador monitorado estabelecer uma conexão de protocolo IP, e (2) no caso de um módulo de segurança com um módulo de interface de dados celulares, a capacidade de o computador monitorado enviar e receber mensagens SMS.

De preferência, a presença e o funcionamento do módulo de segurança são secretos ou não-óbvios ao usuário do computador. No caso de o módulo de segurança não ter a sua própria fonte de alimentação, o sistema como um todo pode ou não ser concebido de modo a fornecer uma energia independente para o módulo de segurança.

Se necessário, uma assinatura de dados é estabelecida para as redes disponíveis para o módulo ou subsistema de segurança. Alternativamente, o serviço é provido no momento exato através de interfaces entre a central de monitoramento e a rede de comunicação.

O módulo de segurança, em conformidade com a presente invenção, habilita serviços robustos de rastreamento de bens e recuperação de roubo, com alguns aspectos comportamentais, um ou mais dos quais podendo ser incorporados em várias modalidades do sistema. Por exemplo, o agente host chama a central de monitoramento em uma programação predeterminada ou após uma mudança interessante dos atributos do computador monitorado, por exemplo, uma mudança no seu endereço de IP, e prefere chamar a central de monitoramento em conexões de rede estabelecidas. O agente host usa conexões de rede que normalmente têm zero ou baixo custo, incluindo as conexões de IP pela Ethernet ou redes WiFi. O agente host e o agente de firmware fazem interface de modo que, quando o agente host está chamando normalmente, apenas o agente host faz chamadas. A este respeito, o agente de firmware é como um sistema de comunicação seguro contra falhas ou de backup.

O agente host e/ou o software de suporte de agente host transfere os atributos do computador monitorado e o sistema OS que normalmente ficaria indisponível para um módulo embutido, incluindo os números de

série do computador, o tipo do sistema operacional host, os aplicativos instalados no sistema operacional host de funcionamento sistema, etc. Esta transferência pode acontecer periodicamente, ou como um resultado de uma mudança em um ou mais atributos.

Quando o agente host não liga por qualquer motivo, ou se encontra desativado, o agente de firmware fará a chamada. Devido à transferência dos atributos do agente host para o módulo de segurança, o agente de firmware será capaz de apresentar um relatório para a central de monitoramento sobre os mesmos atributos que o agente host relata, permitindo que o computador seja identificado e os atributos sejam carregados para a central de monitoramento.

Independentemente de sua capacidade regular de chamada, o agente host é capaz de enviar e receber mensagens para e a partir da central de monitoramento. As mensagens da central de monitoramento podem, por exemplo, indicar que o agente host deve chamar a central de monitoramento de modo a invocar uma medida de proteção de dados. Estas mensagens podem ser através de mensagens SMS.

Além de sua regular capacidade de chamada, o agente de firmware poderá também independentemente enviar e receber mensagens para a/da central de monitoramento. As mensagens da central de monitoramento podem, por exemplo, indicar se o agente de firmware deve despertar o host para que uma medida de proteção de dados possa ser invocada.

Quando uma tecnologia de determinação de localização se encontra disponível no módulo de segurança ou em outro subsistema, o agente host e/ou o agente de firmware poderão relatar esta posição para a central de monitoramento.

Quando o sistema OS do host é reinstalado, o módulo de segurança é detectado através de um recurso plug-and-play ou outra detecção de hardware ou processo de seleção de driver, e o driver, o agente ou o software de suporte para o módulo de segurança poderão ser reinstalados a partir do Windows ou outros meios de instalação de sistema OS ou através de fontes on-line para os drivers, como o Windows Update.

De acordo com uma outra modalidade da presente invenção, um bem a ser protegido, por exemplo, um dispositivo eletrônico, tal como um computador portátil, compreende um agente que é executado a partir do sistema OS do computador portátil, e adicionalmente um módulo de segurança sem fio que pode transmitir e receber, e que pode ser semelhante a um módulo sem fio celular embutido regular. O módulo sem fio inclui um firmware que pode instruir o módulo a chamar uma central de monitoramento independentemente do agente host. O firmware poderá fazer a chamada em um canal de assinante celular regular ou em um canal de segurança dedicado.

A central de monitoramento é habilitada a inicializar uma solicitação de assinatura para um canal de computador adormecido. A vantagem deste recurso é que o usuário não precisará manter uma assinatura de comunicação celular, caso a mesma não tenha sido solicitada para um uso normal do computador portátil por parte do usuário. No caso de um roubo, o usuário poderá informar a central de monitoramento sobre o roubo para que um provisionamento just-in-time de um canal de comunicação sem fio possa ser feito no sentido da recuperação ou para que sejam tomadas medidas para a proteção dos dados.

Os usos comerciais mais importantes da tecnologia apresentada podem incluir a recuperação do roubo de computadores roubados e o gerenciamento de rastreamento de bens de computadores. Uma vez que as características fundamentais da tecnologia devem ser persistentes e difíceis de se remover acidentalmente, até mesmo por usuários autorizados, e de se dispor de um canal de comunicação confiável, que fica adormecido e pode ser acordado, ou recuperável, a tecnologia pode ser utilizada para muitos fins, inclusive para garantir a instalação de aplicativos de qualquer tipo. Os aplicativos que mais se beneficiam de tais recursos são os aplicativos de gerenciamento de sistemas.

Uma vantagem do sistema, quando aplicado a um sistema host, como um computador portátil com uma interface de rádio celular, é que ele poderá se conectar com uma central de monitoramento a qualquer momento e local onde houver cobertura de rede. Ele não precisará esperar que uma

conexão de Internet WiFi ou a fio seja estabelecida. No caso de um módulo acionado independentemente, esta vantagem fica ainda mais evidente, uma vez que a comunicação poderá ser feita sem ter de esperar até que o computador portátil seja ligado. A comunicação com um laptop pode ser feita mesmo que não haja nenhum sistema OS ou que um sistema OS não suportado esteja instalado no sistema do host. Ele poderá resistir a ataques contra a integridade do agente host, além de poder evitar firewalls, os quais poderiam bloquear o agente host.

De acordo com uma outra modalidade da presente invenção, o módulo de segurança pode suportar um canal de comunicação sem fio dedicado apenas para fins de segurança, permitindo que dados e cargas aéreas sejam faturados a um provedor de serviço de recuperação de roubo. Isto permitirá a comunicação, mesmo que o assinante não tenha adquirido um serviço pessoal sem fio ou que o serviço pessoal do assinante seja finalizado por qualquer motivo, inclusive roubo do sistema. A disponibilidade de um canal de segurança dedicado e de canal de assinante permite o desenvolvimento da lógica no sentido de selecionar um canal de comunicação adequado baseado na otimização dos custos tanto para o assinante como para o provedor de monitoramento de segurança. Por exemplo, o canal do assinante poderia ser usado e o assinante faturado até que esse canal se torne indisponível por qualquer motivo.

A recuperação de roubo e o sistema de monitoramento de bens podem incluir ou interagir com um ou mais dentre os vários componentes, recursos e serviços apresentados e patenteados nos Estados Unidos e em outros países, e igualmente cedidos à Absolute Software Corporation. Vide, por exemplo, as Patentes U.S. Nºs 5 715 174, 5 764 892, 5 802 280, 6 244 758, 6 269 392, 6 300 863 e 6 507 914, totalmente incorporadas ao presente documento a título de referência, como plenamente aqui apresentadas.

BREVE DESCRIÇÃO DOS DESENHOS

Para uma melhor compreensão da natureza e vantagens da presente invenção, bem como do seu modo preferido de uso, deve ser feita referência à descrição detalhada a seguir, lida em conjunto com os desenhos

em anexo. Nos desenhos, numerais de referência similares designam peças similares em todos os seus aspectos.

A figura 1 é um diagrama esquemático em blocos funcionais, ilustrando um dispositivo protegido com um módulo de segurança e suas interações, em conformidade com uma modalidade da presente invenção.

A figura 2 é um fluxograma funcional representando esquematicamente o processo de fluxo durante uma operação normal, de acordo com uma modalidade da presente invenção.

A figura 3 é um fluxograma funcional representando esquematicamente o processo de fluxo, quando o agente host está inativo, de acordo com uma modalidade da presente invenção.

A figura 4 é um fluxograma funcional representando esquematicamente o processo de fluxo para as chamadas iniciadas na central de monitoramento, de acordo com uma modalidade da presente invenção.

A figura 5 é um diagrama esquemático representativo dos enlaces de comunicação incluindo as redes por meio das quais o módulo de segurança da presente invenção poderá ser implementado em conformidade com uma modalidade da presente invenção.

DESCRIÇÃO DETALHADA DA MODALIDADE PREFERIDA

A presente descrição é o melhor modo atualmente contemplado para a execução da presente invenção. Esta descrição é feita com a finalidade de ilustrar os princípios gerais da presente invenção e não deve ser tomada em um sentido limitante. O âmbito de aplicação da presente invenção é mais bem determinado com referência às reivindicações em apenso. A presente invenção pode encontrar utilidade em uma variedade de implementações, sem se afastar do âmbito e do espírito da presente invenção, conforme ficará aparente a partir do entendimento dos princípios que subjazem a presente invenção. Com a finalidade de ilustrar as características e funções do módulo de segurança da presente invenção, é feita referência ao monitoramento e recuperação de bens como um exemplo dos serviços, em conjugação com os quais a presente invenção pode ser implantada. Deve-se entender que o módulo de segurança da presente invenção pode ser usada

para outros serviços, tais como as aplicações de gerenciamento, backup e recuperação, operações de exclusão de dados remotos, etc., sem se afastar do espírito e âmbito de aplicação da presente invenção.

As descrições detalhadas que se seguem são apresentadas em grande parte em termos de métodos ou processos, representações simbólicas de operações, funcionalidades e características da presente invenção. Estas descrições e representações de método são os meios utilizados por aqueles versados na técnica de modo a transmitir mais eficazmente a substância de seu trabalho a outros versados na técnica. Um método ou processo implementado por um software é aqui, e de modo geral, concebido para ser uma seqüência coerente de etapas que se conduzem para um resultado desejado. Estas etapas requerem manipulações físicas de grandezas físicas. Muitas vezes, mas não necessariamente, estas quantidades assumem a forma de sinais elétricos ou magnéticos susceptíveis de serem armazenados, transferidos, combinados, comparados, ou de outra forma manipulados. Será ainda apreciado que a linha entre o hardware e o software nem sempre é clara, ficando entendido por parte dos versados na técnica que os processos implementados por um software podem ser incorporados em um hardware, em um firmware, ou em um software, sob a forma de instruções codificadas, como em microcódigos e/ou armazenados em instruções de programação.

Resumo Introdutório do Módulo de Segurança e Aplicação

O módulo de segurança da presente invenção pode ser implantado em um dispositivo host (por exemplo, em um dispositivo eletrônico), que provê um agente secundário que opera em coordenação com o agente host no dispositivo host, mas opera independente do sistema OS do host do dispositivo host de modo a acessar independentemente a interface de rede de comunicação existente no dispositivo host ou uma interface de rede dedicada separada, quando disponível. O sistema geral inclui uma central de monitoramento; um ou mais dispositivos host monitorados; um módulo de segurança nos dispositivos host monitorados; uma ou mais redes de comunicação; uma assinatura para pelo menos uma rede de comunicação. Os dispo-

sitivos host monitorados podem ser dispositivos independentes, tais como os computadores (por exemplo, os computadores portáteis ou de mesa), ou um dispositivo ou subsistema incluído em um sistema. Um dispositivo monitorado compreende um módulo de segurança, um agente host e um software a fim de suportar o agente host que é executado no sistema OS do dispositivo monitorado.

O módulo de segurança da presente invenção pode ser utilizado como um componente ou subsistema, que complementa os aplicativos de rastreamento de bens existentes. Por exemplo, o módulo de segurança pode ser implementado como um componente do AbsoluteTrack e/ou do Computrace desenvolvido pela Absolute Software Corporation, a cessionária da presente invenção. O Computrace é um produto e serviço que rastreia seguramente e recupera bens perdidos ou roubados, e o AbsoluteTrack, vem a ser uma solução para o rastreamento seguro de bens, para o gerenciamento de bens, para a recuperação de bens, para a exclusão de dados, e para a implantação de software, etc., acionado pela plataforma tecnológica do Computrace. O Computrace implanta um agente secreto, que vem a ser um software cliente que reside no disco rígido dos computadores clientes. A Absolute Software Corporation aperfeiçoou ainda mais a plataforma original do agente, provendo um Agente de serviço resistente à violação melhorado de modo a habilitar, suportar e/ou prover vários serviços relacionados ao gerenciamento e proteção de bens (incluindo, sem limitação, o hardware, o firmware, o software, os dados, etc.), incluindo serviços, tais como a exclusão de dados, a proteção por firewall, a criptografia de dados, o rastreamento de localização, a notificação por mensagens, e a implantação e atualizações do software. As funções de serviço podem ser controladas por um servidor remoto. A tecnologia subjacente aos vários produtos e serviços Computrace foram apresentados e patenteados nos Estados Unidos e em outros paises, cujas patentes foram cedidas em conjunto à Absolute Software Corporation. Vide, por exemplo, as Patentes U.S. Nºs 5 715 174; 5 764 892; 5 802 280; 6 244 758; 6 269 392; 6 300 863; e 6 507 914; e suas patentes estrangeiras relacionadas. Os detalhes de um agente persistente e de diversos serviços

relacionados são apresentados no Pedido de Patente copendente U.S. Nº de Série 11/093 180, depositado em 28 de março de 2005 (agora a Publicação de Patente U.S. Nº US2005-0216757; que corresponde à Publicação do Pedido PCT Nº WO 2006/102399); no Pedido de Patente U.S. Nº de Série 11/386 040, depositado em 20 de março de 2006 (agora a Publicação de Patente U.S. Nº US2006-0272020), e o Pedido de Patente U.S. Nº de Série 11/726 352, depositado em 20 de março de 2007 (agora a Publicação de Pedido de Patente U.S. Nº US2007-0234427 A1, que corresponde à Publicação do Pedido PCT Nº WO 2007/109366).

Outras informações relativas ao AbsoluteTrack foram publicadas pela Absolute Software Corporation (por exemplo, o "AbsoluteTrack - Secure Computer Asset Tracking Solution", um documento informal publicado em 25 de abril de 2003). Estes documentos são totalmente incorporados à guisa de referência ao presente documento, como se aqui apresentados na íntegra.

Recuperação de Roubo e Resumo Introdutório do Sistema de Rastreamento de Bens

O rastreamento de bens e a recuperação de roubo vêm a ser um exemplo de serviços que podem ser habilitados com, suportados por e/ou providos com o aplicativo de identificação de dispositivo da presente invenção. O dispositivo ou bem a ser protegido pelo sistema de rastreamento de bens e recuperação de roubo aqui apresentado é referido como um host. O host pode ser um computador portátil, um telefone celular, um Blackberry, um console de jogo eletrônico portátil, um assistente pessoal digital, um dispositivo de entretenimento de áudio ou visual, um equipamento médico, qualquer sistema ou dispositivo que inclua um computador, qualquer outro dispositivo eletrônico ou um rastreador eletrônico dedicado para a obtenção de bens eletrônicos ou não-eletrônicos, tais como veículos motorizados, barcos, ou artigos em trânsito.

Com referência à figura 5, o sistema de rastreamento de bens de acordo com uma modalidade da presente invenção envolve uma arquitetura cliente/servidor, que pode compreender os seguintes componentes principais: (a) um dispositivo host A consistindo, por exemplo, de qualquer dentre

os dispositivos eletrônicos mostrados e implantados com um agente host persistente opcional e um módulo de segurança de acordo com a presente invenção. O agente host e o agente secundário no módulo de segurança são executados de uma maneira coordenada nos dispositivos host A com a finalidade de relatar aplicativos implementados, incluindo, por exemplo, as informações relatadas para, e as instruções recebidas de um servidor remoto a fim de programar o agente host no sentido de suportar e executar uma função desejada; (b) um enlace de comunicação B, como uma rede de troca de informações, podendo incluir as redes de comunicação comutadas, a Internet, uma intranet pública ou privada, as redes de rádio, as redes via satélite, e as redes a cabo; e (c) um sistema de monitoramento host C, que inclui um servidor de monitoramento host 3 que monitora a comunicação entre o dispositivo host A e o sistema de monitoramento host C, que é contatado em uma base regular ou programada pelos dispositivos host, e registra as informações dos dispositivos host. O servidor de monitoramento também provê instruções ao host sobre quais ações realizar, inclusive que ações o host deve executar, que dados coletar e a próxima hora de chamada programada do host.

De acordo com a presente invenção, o sistema de monitoramento host C é configurado de modo a se comunicar com o agente host no dispositivo host A com o agente secundário no módulo de segurança do dispositivo host A, que remotamente determina a identidade dos dispositivos host que são monitorados (por exemplo, ao avaliar os pontos de dados coletados utilizando o aplicativo de coleção de atributos de dispositivo residente nos dispositivos host, conforme apresentado no Pedido de Patente U.S. Nº de Série 11/726 352, depositado em 20 de março de 2007 (agora a Publicação de Pedido de Patente U.S. Nº US2007-0234427 A1; que corresponde à Publicação de Pedido PCT Nº WO 2007/109366). Os dispositivos host A entram em contato com o servidor de monitoramento através do enlace de comunicação B. O sistema de monitoramento de host C pode incluir um portal de relatório e administração, que oferece aos clientes, aos administradores e aos provedores de serviço de rastreamento de bens a capacidade de visua-

lizar dados e gerenciar as funções do servidor de monitoramento e dos dispositivos host.

Com a exceção do módulo de segurança da presente invenção e de sua integração nos dispositivos host, cada um dos componentes mostrados na figura 5 foi apresentado em sua totalidade no Pedido de Patente copendente U.S. Nº de Série 11/386 040, depositado em 20 de março de 2006 (agora, a Publicação de Pedido de Patente U.S. Nº US2006-0272020; que corresponde à Publicação de Pedido PCT Nº WO 2006/102399).

Os dispositivos host A que são implementados com o módulo de segurança da presente invenção de acordo com a presente invenção podem ser seletivamente operados, ativados ou configurados por um programa, aplicativo, rotina e/ou uma sequência de instruções e/ou lógica armazenadas nos dispositivos, além dos sistemas operacionais host residentes nos dispositivos. Em suma, o uso dos métodos descritos e sugeridos no presente documento não se limita a uma configuração de processamento específica. A título de exemplo e não de limitação, a presente invenção é descrita com referência aos exemplos de aplicações e implementações com referência a um computador laptop ou a um computador notebook, como o dispositivo host A (o computador A1 é esquematicamente representado como um dispositivo de mesa, mas poderá, ainda, compreender um dispositivo computacional portátil).

Os enlaces de comunicação B incluem qualquer forma de redes de troca de informações nas quais a presente invenção pode ser implementada para o rastreamento de bens. A rede de troca de informações acessada pelo dispositivo host, incluindo o módulo de segurança de acordo com a presente invenção pode envolver, sem limitação, as redes distribuídas de troca de informações, tais como as redes de computador públicas e privadas (por exemplo, a Internet, a Intranet, a rede WWAN, a rede WAN, a rede LAN, etc.), as redes de valor agregado, as redes de comunicação (por exemplo, as redes com fio ou sem fio), as redes de difusão, as redes a cabo, a rede celular, as redes de rádio, e uma combinação homogênea ou heterogênea de tais redes. Conforme será apreciado pelos versados na técnica, as redes

incluem tanto um hardware como um software, e podem ser visualizadas tanto isoladamente, como em conjunto, de acordo com qual descrição seja mais útil para um propósito em particular. Por exemplo, a rede pode ser descrita como um conjunto de nós de hardware que podem ser interconectados por um aparelho de comunicação, ou, de maneira alternativa, como o aparelho de comunicação, ou ainda, de maneira alternativa, como o próprio aparelho de comunicação com ou sem os nós. Será ainda apreciado que a linha entre um hardware, um firmware e um software nem sempre é bem definida, ficando entendido por aqueles versados na técnica que tais redes e o aparelho de comunicação, ou os componentes de uma plataforma de tecnologia de agente persistente, envolvem aspectos relativos a um software, a um firmware e a um hardware.

Rastreamento de Bens e Recuperação de Roubo com o Emprego de um Módulo de Segurança

Serão descritas a seguir, em mais detalhes, as várias etapas de um sistema de rastreamento de bens e recuperação de roubo que emprega um módulo de segurança (e, em particular, um módulo de segurança sem fio), os dispositivos compreendendo um módulo de segurança e seus modos de operação. Como um exemplo descritivo, um computador laptop é utilizado como o dispositivo a ser protegido e, no presente pedido, é definido como o host para o módulo de segurança sem fio e para os diversos agentes de software e firmware incluídos no sistema de segurança. As peças do sistema incluem um host, o módulo de segurança, um agente host persistente, um agente de firmware; um software de suporte; e uma central de monitoramento.

O software de suporte, sob a forma de instruções legíveis em computador de ou em um meio legível em computador, fica armazenado no host. O software de suporte compreende um driver e uma camada de interface de programas aplicativos (API) a fim de fazer a interface do módulo sem fio com o host. Tanto o driver como a interface API se baseiam em um driver padrão para um módulo celular sem fio, porém estendidos das seguintes maneiras. A interface API é estendida de modo a suportar as interfaces API

adicionadas requeridas para interface com o agente de firmware. A interface API é estendida de modo a suportar o acesso ao armazenador de atributos no módulo de segurança. A interface API é estendida de modo a permitir que apenas os aplicativos confiáveis invoquem as funções sensíveis do módulo de segurança, incluindo cada uma das extensões de interface API acima. Quando o módulo de segurança suporta o uso de um canal de comunicação de segurança dedicado (OTA), a interface API e o driver são estendidos de modo a permitir que os aplicativos confiáveis criem, gerenciem e usem o canal de comunicação de segurança dedicado.

Interações Entre Componentes

Três componentes principais interagem no sentido de facilitar as funções de rastreamento de bens e recuperação de roubo, incluindo um módulo de segurança, um agente host primário e uma central de monitoramento.

A. Módulo ou Subsistema de Segurança

Os atributos gerais do módulo ou subsistema de segurança são um agente secundário, sob a forma de um agente de firmware, por exemplo, ou de outra forma, carregado a partir do armazenador de aplicativo persistente, uma interface de rede e um armazenador de dados do qual o agente de firmware lê ou para o qual o agente de firmware escreve.

O agente secundário é habilitado com funções específicas, dedicadas a se coordenar com o agente host a fim de se comunicar para fora, e com outras funções relacionadas, descritas em mais detalhes no presente documento. O agente de firmware do módulo ou subsistema de segurança pode ser executado no processador específico de um módulo celular sem fio, mas pode também residir em qualquer outro lugar no computador monitorado. Outros locais adequados incluem um processador separado na placa mãe ou embutido separado da placa mãe. O agente de firmware tem acesso ao armazenador de dados persistente ao qual ele pode ler ou escrever.

O firmware, quer localizado no módulo sem fio ou em outro lugar qualquer, poderá ou não ser estendido de modo a suportar um canal de comunicação de segurança OTA dedicado. O firmware inclui um agente de

firmware, que poderá acionar uma chamada sem fio para uma central de monitoramento independentemente de um agente host implementado no sistema OS. Ao usar os atributos armazenados no armazenador de dados persistente ao qual ele tem acesso, o agente de firmware poderá atuar como um substituto do agente host.

O firmware de interface de host suporta os mecanismos para configurar e usar o canal de comunicação de segurança; para fazer interface com e controlar o agente de segurança de firmware; e armazenar os atributos do computador host no módulo de segurança. Em cada caso, estes próprios mecanismos são protegidos com medidas de segurança a fim de garantir que o canal de comunicação de segurança só possa ser utilizado por aplicativos autorizados.

O módulo de segurança compreende uma ou mais interfaces de rede ou acesso compartilhado às interfaces do host. O módulo de segurança pode ter uma interface de rede dedicada às comunicações relacionadas à segurança. Uma ou mais dentre as interfaces de rede pode ser uma interface de rede WWAN.

O módulo de segurança compreende um hardware e um software de interfaces opcionais, permitindo que o módulo de segurança provoque a inicialização ou a continuação do sistema OS do host.

De acordo com a presente invenção, existem diversas formas físicas diferentes que o módulo de segurança sem fio pode assumir, como se segue:

(i) Módulo de Dados de Rede Remota Sem Fio (WWAN)

Este módulo vem a ser um módulo de hardware que pode ser incorporado em hosts, como os computadores altamente portáteis. Ele implementa funções similares a de um módulo celular sem fio regular embutido. Com efeito, a menos que os aspectos de segurança da presente invenção estejam habilitados, o módulo poderá operar unicamente como um módulo celular sem fio regular embutido.

O módulo de segurança sem fio pode suportar um ou dois canais de comunicação independentemente faturáveis. Uma forma de se obter

dois canais independentemente faturáveis é quando o módulo se comporta como dois dispositivos celulares independentes, com identificadores de equipamento separados. Para comutar entre canais, o módulo tira o registro da rede corrente à qual o mesmo se inscreveu e, em seguida, volta a se registrar na rede, ou em uma rede diferente, com um identificador ID de equipamento diferente. De maneira alternativa, o módulo pode simplesmente suportar duas bandas base totalmente separadas, cada qual registrando diferentes identificadores de equipamento. De outra maneira alternativa, um mecanismo completamente diferente pode ser usado de modo a permitir um faturamento independente das comunicações. Em uma outra alternativa, o módulo pode ser configurado ou configurável de modo a suportar os futuros protocolos OTA que permitem que um módulo celular sem fio com um identificador de equipamento a fim de suportar múltiplos canais de dados independentemente faturados.

Vários laptops encontram-se disponíveis a partir da OEM e incluem modems celulares (módulos móveis de banda larga aka, etc.). Por exemplo, os módulos www.dell.com, www.hp.com, www.lenovo.com, etc. Estes módulos têm geralmente dois processadores (mais comumente agora na mesma matriz). (Vide, ainda, a Síntese do Produto publicado pela Broadcom Corporation EDGE/GPRS/GSM Single-Chip Multimedia Baseband Processor; Publicação Nº BCM2133-PB07-D1; de 30/11/06; http://www.broadcom.com/collateral/pb/2133 -PB07-R.pdf). O agente de firmware é tipicamente executado no "processador específico" do módulo.

(ii) Subsistema de Rede WWAN

Este subsistema tem a mesma funcionalidade que o módulo mencionado no item (i), com exceção de que o chip ou chips do hardware se localiza na placa mãe e não no módulo.

(iii) Subsistema de Segurança

Neste caso, a funcionalidade do módulo ou subsistema de segurança é incorporada em um processador, que é separado do processador principal do laptop. Por exemplo, o mesmo pode ser incorporado em um processador separado que pode injetar e filtrar pacotes na e para fora da con-

troladora de rede do host. Um exemplo de tal modalidade pode compreender o agente secundário executado como um serviço na estrutura de firmware da Máquina de Gerenciamento dentro da arquitetura AMT da Intel: (Vide o documento Architecture Guide: Intel Active Management Technology, publicado em 19 de setembro de 2007. http://softwarecommunity.intel.com/articles/eng/1032.htm.) Na arquitetura AMT, o segundo processador é executável com uma força auxiliar.

(iv) Implementação da Virtualização

Neste caso, a funcionalidade do módulo ou subsistema de segurança é executada em um ambiente virtual no processador principal do computador. O sistema OS do host é executado conforme o normal e desconhece totalmente o ambiente de segurança e o agente de firmware. (Para maiores informações sobre virtualização, vide o documento An overview of Virtualization: Introduction to Virtualization - Overview of Virtualization and the Most Common Types of Virtualization; http://www.virtualization.org/ Virtualization/Introduction_to_VirtualizatioN.html). O "agente de firmware" pode ser executado como uma parte do hipervisor ou em uma instância do sistema OS totalmente separada.

B. Agente host

De acordo com uma modalidade, o agente host é um módulo cliente à prova de violação incorporado no host. No presente pedido, o mesmo refere-se a um agente executado a partir do sistema OS do host. O sistema OS do host suporta a execução de aplicativos do usuário para o dispositivo, por exemplo, um computador que executa o sistema OS da Microsoft, um telefone celular que executa o sistema OS da Symbian, etc. Na técnica anterior, o agente host ou seus componentes pode ser referido como um agente, um agente inteligente, um agente transparente, um agente segmentado, um agente persistente, um agente de serviço, um agente de serviço à prova de violação, um agente de aplicativos, um agente de rastreamento, um agente secreto, um agente extensível, um agente de chamada, um agente de driver de função total, um agente de driver parcial, um agente do Computrace ou outros termos similares.

O agente host chama a central de monitoramento periodicamente ou quando ocorre uma mudança interessante no computador monitorado. Durante a chamada, ele poderá relatar os atributos do computador monitorado, e poderá incluir atributos no sentido de estabelecer uma conexão de dados celulares, caso necessário.

O agente host detecta a presença do módulo ou subsistema de segurança, instala o necessário software de interface e suporte e faz interface e controla o mesmo. Isto inclui um comportamento de chamada de sincronização de modo que normalmente apenas o agente host chame a central de monitoramento, e não o agente de firmware. Por outro lado, pode ser desejável permitir que o agente de firmware chame a central de monitoramento no momento de se verificar a correta operação do sistema. O mesmo também se aplica à transferência de atributos para o agente host.

Quando o módulo de segurança inclui uma interface celular, o agente host poderá enviar e receber mensagens SMS usando esta interface. A central de monitoramento pode solicitar ao agente host para iniciar uma conexão de dados celulares através de uma mensagem SMS.

O agente host também provê informações suficientes para uma central de monitoramento para que a central de monitoramento ative uma assinatura para um canal de comunicação de segurança, se e quando tal canal se torna necessário. Isto inclui, por exemplo, ao se prover um único identificador de equipamento para um módulo sem fio.

Em outras modalidades da presente invenção, o agente usará o canal de comunicação de segurança somente quando necessário, para relatar a localização de um host, ou para a realização de tarefas urgentes ou importantes. Em um modo, o canal de comunicação de segurança é empregado somente quando um canal de assinante se encontra indisponível por qualquer motivo, de tal forma que as despesas de serviço e de suporte incorridas por uma central de monitoramento sejam mantidas a um mínimo. Em uma modalidade, o agente é configurado de modo a estabelecer uma conexão de dados celulares de acordo com circunstâncias especiais, por exemplo, quando as tentativas para se conectar através de internet não foram

bem sucedidas por mais de um período de tempo predeterminado. Outros modos operacionais podem também ser concebidos.

Em uma modalidade, o agente suporta as chamadas iniciadas por uma central de monitoramento ao invés de fazer a central de monitoramento esperar por uma chamada programada a partir do host. A central de monitoramento pode iniciar uma chamada de dados de modo a permitir que o agente se comunique por uma rede celular ao invés de pela internet. Por motivos de otimização de custos, a central de monitoramento pode transmitir uma chamada de Serviço de Mensagem Curta (SMS) que aciona o agente de firmware no sentido de inicializar uma chamada originada por um host. Esta chamada SMS, ou um tipo de chamada basicamente similar, pode fazer com que o agente de firmware desperte o host e permite que o agente host faça a chamada.

O agente pode se encontrar em um modo passivo, em um modo ativo ou em um modo alerta. No modo passivo, o agente está presente, porém não faz nada até que ativado pelo usuário que estabelecer uma assinatura para o monitoramento de segurança ou rastreamento de bens. No modo ativo, o agente chama a central de monitoramento a intervalos regulares, predeterminados ou aleatórios. No modo alerta, o host foi roubado e o agente recebe uma instrução por parte da central de monitoramento no sentido de chamar com mais frequência ou de realizar tarefas de proteção, tais como a criptografia de dados.

C. Central de Monitoramento

De acordo com a presente invenção, a central de monitoramento é configurada de modo a se comunicar a interface de rede do dispositivo host, cujo acesso é gerenciado pelo agente host em coordenação com o agente secundário no módulo de segurança. As centrais de monitoramento são, por vezes, também referidas por meio do uso de outros termos, incluindo estação remota, servidor remoto, servidor, sistema de monitoramento de host, sistema host, sistema host remoto e servidor de monitoramento.

De acordo com uma modalidade da presente invenção, uma típica central de monitoramento pode compreender servidores e software de

chamada, servidores da web e aplicativos da web, servidores de banco de dados ou bancos de dados, sistemas de autenticação, sistemas administrativos e sistemas de processamento de back end. A central de monitoramento pode receber as chamadas de agentes host por meio de vários serviços de suporte, tais como o protocolo IP ou pela rede PSTN, e pode identificar computadores, determinar o seu nível de licenciamento e registrar seus atributos e localização, instalar e atualizar o software de computadores monitorados, e configurar serviços de exclusão de dados e ferramentas de recuperação de roubo. Uma central de monitoramento pode prover uma interface de web para que usuários gerem relatórios de seus bens monitorados e suas localizações.

Além disso, a central de monitoramento do presente sistema de rastreamento de bens e recuperação de roubo compreende um ou mais recursos novos. Estes incluem, por exemplo, interfaces com gateways para a troca de mensagens SMS, o que possibilita a iniciação de operações de recuperação de roubo antes de a central de monitoramento esperar que os dispositivos a serem protegidos chamem de acordo com a sua programação. Um benefício adicional é que a central de monitoramento poderá potencialmente se comunicar com computadores off-line. Uma outra vantagem extra é que a central de monitoramento poderá potencialmente se comunicar com computadores desligados, mas possuem módulos de segurança separadamente acionáveis através de uma chamada para despertar.

A central de monitoramento pode ser uma estação de serviço de monitoramento com uma equipe de trabalho. Uma pluralidade de sistemas de monitoramento pode ser distribuída através das redes de comunicação, por exemplo, em diferentes regiões geográficas.

Com relação ao módulo de segurança de acordo com a presente invenção, um servidor de central de monitoramento compreende um processador, um disco rígido e controladora de disco rígido, ou outros meios de armazenador de dados, e é configurado de modo a executar uma ou mais dentre as funções adicionais descritas abaixo. Um teclado e tela podem ser operacionalmente conectados ao servidor de modo a permitir a entrada de

dados no e a leitura de dados pelo servidor, e possibilitar que um operador interaja com um servidor de monitoramento.

Uma primeira função adicional de uma central de monitoramento é detectar a presença do módulo de segurança durante uma chamada de agente host e configurar a mesma e sincronizar o comportamento da chamada do agente host e do agente de firmware.

Uma segunda função adicional de uma central de monitoramento é coletar e armazenar os novos atributos coletados dos clientes com os módulos de segurança. Estes novos atributos incluem, por exemplo, o identificador de equipamento para o módulo de segurança.

Uma terceira função adicional de uma central de monitoramento é ativar uma assinatura para o canal de comunicação de segurança, quando necessário, em momentos apropriados. Este processo de ativação requer interfaces com os sistemas de portadoras. De maneira alternativa, na notificação de um proprietário de um dispositivo rastreado que foi roubado, a equipe de trabalho de uma central de monitoramento poderá contatar, via telefone, e-mail, fax ou outro método, a companhia de telecomunicação no sentido de estabelecer uma assinatura para o módulo sem fio do dispositivo rastreado que foi roubado.

Uma quarta função adicional da central de monitoramento é iniciar chamadas para os computadores rastreados. Esta função é particularmente útil quando o dispositivo rastreado é notificado como roubado. Ao invés de esperar que o dispositivo rastreado chame a central de monitoramento em sua vez programada seguinte, o dispositivo rastreado pode ser chamado imediatamente e o agente host colocado em modo de alerta. Esta tecnologia pode ser implementada através de uma mensagem SMS ou outro serviço com capacidades similares que possibilitem uma entrada de comunicação com o computador monitorado.

Uma quinta função da central de monitoramento é registrar informações de localização adicionais, relativas à localização do dispositivo rastreado, ou informações que possam ser usadas para inferir a localização do dispositivo rastreado. Estas informações podem incluir as coordenadas

coletadas a partir de um transceptor de sistema GPS embutido no módulo de segurança ou de uma unidade de sistema GPS separada do módulo de segurança; os identificadores ID das torres celulares visíveis e suas respectivas forças de sinal; os endereços MAC e as forças de sinal dos roteadores WiFi visíveis. No caso em que a localização do dispositivo é provida diretamente, por exemplo, no caso do sistema GPS, a localização é armazenada diretamente no banco de dados. Quando a localização é inferida a partir de atributos coletados, por exemplo, dos endereços MAC ou das forças de sinal dos roteadores WiFi visíveis, a central de monitoramento faz interface com um sistema de modo a inferir a localização do computador monitorado.

Modalidade Exemplar

As figuras 1 a 4 ilustram um exemplo da presente invenção aplicada no sentido de rastrear um bem (por exemplo, um dispositivo a ser protegido) que é rastreado por um usuário que instalou um agente no bem, e o bem chama uma central de monitoramento.

O dispositivo a ser protegido, ou host, é um laptop 10. Alguns componentes e módulos do laptop são mostrados no sentido de ajudar no entendimento da presente invenção, e outros foram omitidos para fins de clareza. O agente host 14 é mostrado residindo no OS 13, juntamente com outros recursos, tais como os serviços de pilha de rede/OS 15 e outros drivers 18. O agente host tem um módulo de persistência 11 residente no sistema BIOS 12. Este módulo de persistência restaura 51 a pré-inicialização do agente host, se necessário. O agente host 14 pode ser instalado no host através de um meio de distribuição legível por computador 40, no qual são executadas as instruções legíveis por computador 41 que formam um instalador de arquivos MSI juntamente com necessários arquivos e código para a instalação do agente host. Outros tipos de meio legível em computador podem ser utilizados. É também instalado dentro do OS um driver de módulo 16 que permite que o agente host interaja e controle o módulo de segurança celular sem fio 19. O driver de módulo 16 pode incluir um agente compactado 17 e pode ser configurado de modo a restaurar 52 o agente host, caso necessário, provendo, assim, um nível extra de autorreparação do agente. O

agente host permite 34 a persistência baseada no driver. O driver de módulo 16 compreendendo o agente compactado 17 pode ser instalado no OS a partir de um meio legível por computador 42, que carrega as instruções legíveis por computador 43 que formam o instalador driver de módulo e o necessário código de driver e arquivos, e uma versão compactada do agente host 44. O driver de módulo sem fio e o agente compactado podem também ser instalados através de uma atualização Microsoft 45 que inclui o necessário código de driver 46 e o agente compactado 47. De maneira alternativa, o agente host pode também ser diretamente instalado durante a instalação do sistema operacional ou por meio do Windows Update. O laptop 10 também inclui uma interface de Ethernet 24, uma interface de rede WLAN 23 e um WiFi ou outro modem 22.

O módulo de segurança celular sem fio 19 compreende um agente de firmware 21 e um dispositivo armazenador de dados não-volátil 20. Embora o agente de firmware 21 e o dispositivo armazenador de dados não-volátil 20 tenham sido mostrados como localizados no módulo sem fio 19, os mesmos podem alternativamente se situar em qualquer parte no laptop, juntos ou separados um do outro. O agente de firmware faz com que os atributos do computador, tais como os detalhes de um software instalado, fiquem eletronicamente armazenados no dispositivo armazenador de dados 20. Uma fonte de alimentação opcional 25 é operacionalmente conectada ao módulo de segurança sem fio a fim de permitir que o agente de firmware e o módulo de segurança sem fio operem quando o host é desligado ou não está conectado a uma fonte de alimentação.

O agente host 14 é configurado de modo a fazer interface com e controlar o módulo de segurança 19 e/ou o agente de firmware 21. O agente host 14 e o agente de firmware 21 são configurados de modo a recuperarem as informações de localização quando uma tecnologia de determinação de localização é inclusa no sistema. O agente de firmware só chamará se o agente host não chamar. Por exemplo, o agente de firmware chamará caso o agente host não execute "ping" ao agente de firmware em um período de tempo limite configurável.

Quando um usuário ou proprietário 73 do laptop toma conhecimento de que o laptop foi roubado, o usuário 73 entra em contato com a central de monitoramento 71, por telefone, fax, e-mail ou qualquer outro método disponível. O fato de o laptop ter sido roubado é registrado em um banco de dados de um servidor 71 da central de monitoramento, ou manualmente por um membro da equipamento de trabalho da central de monitoramento ou automaticamente quando a notificação é feita através de uma conexão da internet ou sistema de secretária eletrônica automática.

Se não se deseja aguardar a próxima chamada programada por parte do agente host, a central de monitoramento poderá tentar se comunicar com o host e/ou com o agente de firmware através de transmissão de uma mensagem SMS. Esta mensagem instrui o agente host e o agente de firmware a chamar. Uma vez que o agente host e o agente de firmware recebem a mensagem quase ao mesmo tempo, o agente de firmware aguarda um tempo limite configurável para saber se o agente host chamará. Caso não chame, o agente de firmware criará uma conexão de dados celulares e chamará.

Se não há uma assinatura de dados celulares para o computador monitorado, uma assinatura poderá ser configurada por um elemento da equipamento de trabalho de monitoramento, que contata uma empresa operadora de provedor de rede celular 72 e provê a mesma com um identificador de equipamento para o módulo sem fio, ou isto pode ser feito automaticamente através de interfaces programáticas com um ou mais operadores de redes celulares. Uma assinatura será provavelmente definida depois de um laptop ter sido roubado ou uma solicitação de exclusão de dados ter sido submetida.

A figura 2 é um fluxograma, representando esquematicamente o processo usual com o qual o agente host 14 e o agente de firmware 21 operam, juntamente com sua interação com a central de monitoramento 70. Quando o agente host é executado, depois de verificar o término de sua execução, ele entra em um curto período de espera 200, que pode ser definido em qualquer número predeterminado. Para fins de exemplo ilustrativo

somente, o número pode ser definido em 15 minutos. Após este período de espera, o agente host faz interface 210 com o agente de firmware, que armazena 211 os atributos e a próxima hora de chamada do agente de firmware 212 na memória não-volátil à qual ele tem acesso. A próxima hora de chamada do agente de firmware é tipicamente ajustada a algum número no futuro além do momento seguinte no qual o agente fará interface com o agente de firmware. Porém, caso o agente não tenha conseguido chamar a central de monitoramento em um período estendido, ele poderá indicar ao agente de firmware de que ele deve tentar chamar imediatamente. Os atributos armazenados podem incluir os atributos do OS e os detalhes dos programas instalados no computador.

O agente em seguida verifica se é o momento de chamar a central de monitoramento. O momento de chamar a central de monitoramento pode ser definido para ser a cada 24 horas, por exemplo. Se ainda não for o momento de chamar, o agente host retorna para o modo de espera 200. Se passa o tempo de chamar, o agente host verifica se uma conexão de internet se encontra disponível, e, caso positivo, faz uma chamada 203 para a central de monitoramento através da internet. Antes de chamar, a central de monitoramento fica em um estado de espera 206, no qual ela fica aguardando que uma chamada feita seja recebida. Ao receber a chamada 203, a central de monitoramento processa 207 a chamada, após o que volta a um estado de espera para uma chamada subsequente. Se não existe nenhuma conexão de internet disponível, o agente host verifica se uma conexão celular se encontra habilitada 204, e, caso positivo, ele cria uma conexão de dados celulares 205, a qual utilizará para chamar a central de monitoramento 203.

Se a chamada não consegue se completar 208, o agente host volta para um estado de curta espera 200, e repete o processo descrito. Quando a chamada é bem sucedida, o agente host salva 209 a hora para a sua próxima chamada.

Durante uma chamada bem sucedida, a central de monitoramento consegue registrar a localização e a identidade do computador que cha-

ma, e prover outras instruções para o agente host. Outras instruções para o agente host podem ser no sentido de iniciar um processo de exclusão de dados, uma atualização de programa ou uma mudança de chave de criptografia, e podem incluir ainda instruções a serem executadas após o término da chamada.

Se há um canal celular de usuário e ainda um canal de segurança dedicado sem fio, o agente host poderá ser configurado de modo a chamar o canal de usuário antes de tentar se conectar ao canal de segurança dedicado. O agente host poderá, ao invés de ser configurado para chamar o canal de segurança antes de tentar se conectar com o canal de usuário. De maneira alternativa, a escolha do canal pode ser controlada por um algoritmo para a minimização de custo.

A figura 3 é um fluxograma que representa esquematicamente o processo do agente de firmware 21 no caso em que o agente host 14 se encontra inativo. Isto pode ocorrer quando o computador está desligado, não há conexão com a internet ou o agente host se encontra de alguma forma desabilitado. No caso em que o computador está desligado, o módulo de segurança deve ser autoalimentável.

No caso de um agente host inativo, o agente de firmware fica em um curto período de espera 300. Após este período de espera, o agente de firmware verifica 301 se passou o tempo para chamar a central de monitoramento 70. Caso este tempo não tenha passado, o agente de firmware retorna para o estado de espera 300. Caso já tenha passado o tempo de chamar, o agente de firmware cria a conexão de dados celulares 302, que utiliza para chamar 303 a central de monitoramento. Antes da chamada, a central de monitoramento fica em estado de espera 304, no qual fica aguardando que uma chamada de entrada seja feita. Ao receber uma chamada 303, a central de monitoramento processa 305 a chamada, após o que retorna para um estado de espera para uma chamada subsequente.

Se a chamada não consegue ser feita 306, o agente de firmware volta ao estado de curta espera 300, e repete o processo descrito. Se a chamada é bem sucedida 307, o agente de firmware armazena os atributos

e a hora da próxima chamada 308 na memória não-volátil à qual ele tem acesso. Os atributos armazenados podem incluir os atributos do sistema OS e os detalhes dos programas instalados no computador.

A figura 4 é um fluxograma que representa esquematicamente o agente host 14 e o agente de firmware 21 em um período de espera, uma vez que não há uma hora programada para a chamada, mas se deseja fazer uma chamada para o computador. Por exemplo, este pode ser o caso no qual o computador foi roubado. Inicialmente, o agente host, o agente de firmware e a central de monitoramento 70 ficam em um estado de espera. Quando a central de monitoramento é informada que o computador foi roubado 400, a mesma verificará 401 se existe uma assinatura de dados sem fio, e, caso positivo, faz uma chamada 404 para o host e/ou para o agente de firmware. Se não há assinatura do computador para um provedor de comunicação sem fio, a central estabelecerá uma assinatura 403 utilizando as informações de identificador ID armazenadas ou de outra forma providas 402 relativas ao identificador de equipamento único do módulo sem fio dentro do computador, e, em seguida, faz uma chamada sem fio 404. A fim de estabelecer uma assinatura, a central de monitoramento poderá contatar uma empresa provedora de telecomunicação, de uma forma automática ou manualmente.

A chamada sem fio 404 feita pela central de monitoramento pode ser uma chamada SMS. Quando o agente host se encontra inativo 408, por exemplo, se o computador estiver desligado, ou se o agente host estiver danificado, o agente de firmware aceitará a chamada e processará a mensagem SMS 409. No entanto, quando o agente host se encontra ativo, ele mesmo processará sozinho a chamada SMS 410.

No caso em que o agente host se encontra ativo, a chamada SMS 410 instrui o agente host para chamar a central de monitoramento. Quando a chamada SMS finaliza 411, 405, a central de monitoramento entra em um estado de espera 406 para uma chamada de entrada do dispositivo protegido e o agente host verifica 412 se há uma conexão de internet. Caso positivo, o agente faz uma chamada baseada na internet 414 para to a cen-

tral de monitoramento, porém, caso contrário, ele criará uma conexão celular 413 através da qual chamará 414 a central de monitoramento. A central de monitoramento processa a chamada 407 e, em seguida, retorna para uma estado de espera 406. Após uma chamada bem sucedida, o agente host armazena a próxima hora quando precisará chamar a central de monitoramento, que, no caso de um computador roubado, poderá ser mais cedo do que quando não roubado. Para fins de exemplo, apenas, a próxima hora de chamada pode ser definida para ocorrer em um tempo de 15 minutos. O agente host faz interface 419 com o agente de firmware, que armazena 422 os atributos e a próxima hora de chamada do agente de firmware 421 na memória não-volátil à qual tem acesso. Uma hora de chamada exemplar seria em de um tempo de 25 minutos. Em seguida, o agente host entra em um estado de espera 200, após o que seguirá o procedimento conforme mostrado na figura 2.

No caso onde o agente host se encontra inativo, o agente de firmware interpreta a chamada SMS 409 como uma instrução para chamar a central de monitoramento. A chamada SMS se finaliza 415 e, então, o agente de firmware cria uma conexão de dados celulares 416, através da qual chama a central de monitoramento 417. A central de monitoramento processa a chamada 407 e, em seguida, volta a um estado de espera 406. A chamada pode envolver, por exemplo, uma instrução para o agente de firmware ligar o computador e/ou despertar o agente host.

Após ou durante uma chamada bem sucedida, o agente de firmware armazena os atributos e a próxima hora de chamada do agente de firmware 421 na memória não-volátil à qual tem acesso. O agente de firmware, em seguida, prossegue em um estado de espera 300, e continua o processo descrito na figura 3.

Modalidades Alternativas

Uma modalidade alternativa concebida é a integração total do módulo de segurança sem fio na placa-mãe do sistema host. Isto efetivamente elimina a possibilidade de desabilitar o módulo de segurança através da remoção física do módulo.

A tecnologia descrita não se limita aos meios de comunicação celulares sem fio, podendo empregar outras tecnologias sem fio ou móveis, incluindo uma rede pessoal (PAN), uma rede local sem fio (WLAN) ou as tecnologias baseadas em satélite.

Em uma outra modalidade, o módulo sem fio pode ser capaz de comunicações WiFi e/ou WIMAX e/ou celulares sem fio.

O módulo de segurança pode ser implementado utilizando técnicas de virtualização, nas quais o agente de firmware é executado em um ambiente virtual no processador principal do computador e compartilha as interfaces de rede do sistema de uma maneira completamente desconhecida ao OS principal do computador.

O módulo de segurança sem fio pode ser alimentado por meio de uma fonte de alimentação independente. Esta pode ser da forma de uma bateria dedicada ou simplesmente por meio de conexões independentes com as fontes de alimentação principais do laptop. A vantagem de tal configuração é que o agente de firmware poderá se comunicar mesmo que o sistema host do computador esteja desligado.

No caso de um módulo independentemente energizado, o módulo de segurança sem fio poderá ser capaz de despertar o sistema host. Quando este é o caso, a central de monitoramento poderá se comunicar com o agente de firmware e despertar o computador host a fim de executar, por exemplo, uma operação de proteção de dados.

Os administradores de sistema são também capazes de determinar a localização física dos sistemas rastreados. Eles poderão também por em execução diretrizes de base geográfica, por exemplo, o computador X não pode ser levado para fora de um limite geográfico definido. O agente poderá chamar a central de monitoramento todas as vezes que ocorrer uma mudança de local do laptop detectada, como também chamar de acordo com uma programação predeterminada. De maneira alternativa, ele poderá chamar cada vez que detectar que o mesmo se encontra em uma nova localização ao invés de em local diferente. As informações de localização podem ser providas por meio de uma triangulação celular, de uma triangulação de

força de sinal WiFi, de técnicas de etiquetagem de identificação RFID, de pesquisa de protocolo IP ou de dispositivos de sistema GPS.

As modalidades descritas acima provêm módulos de segurança que podem ser efetivamente integrados em um dispositivo host, que se coordena com o agente host de modo a se comunicar com um site externo. As modalidades do módulo de segurança acima descritas podem ser estendidas para a proteção de vários tipos de dispositivos, sistemas, e subsistemas, não limitados às modalidades estruturais e de processo acima descritas, sem se afastar do âmbito de aplicação e espírito da presente invenção. Sendo assim, o módulo de segurança da presente invenção não deve ficar restrito aos específicos algoritmos de implementação.

O processo e o sistema da presente invenção foram descritos acima em termos de módulos funcionais no formato de diagramas em blocos e de fluxogramas. Deve-se entender que, a menos que de outra forma aqui apresentado, uma ou mais funções podem ser integradas em um único dispositivo físico ou um módulo de software em um produto de software, ou uma ou mais funções podem ser implementadas em dispositivos físicos separados ou os módulos de software em um único local ou distribuídos em uma rede, sem se afastar do âmbito de aplicação ou espírito da presente invenção.

Deve-se apreciar que a apresentação detalhada da real implementação de cada módulo não se faz necessária para o entendimento da presente invenção. A implementação em questão é bem-conhecida dentro da habilidade rotineira de um programador ou de um engenheiro de sistema, dada a apresentação dos atributos de sistema, da funcionalidade e da interrelação dos diversos módulos funcionais do sistema. Uma pessoa versada na técnica, com a aplicação de uma capacidade simples, poderá praticar a presente invenção sem indevida experimentação.

Embora a presente invenção tenha sido descrita com relação às modalidades descritas em consistência com as mesmas, ficará aparente aos versados na técnica que várias modificações e aperfeiçoamentos poderão ser feitos sem se afastar do âmbito de aplicação e espírito da presente in-

venção. Por exemplo, o aplicativo de extração de informação pode ser facilmente modificado no sentido de acomodar diferentes processos ou outros processos de modo a oferecer ao usuário uma flexibilidade extra para navegação na web. Por conseguinte, deve-se entender que a presente invenção não se limita às modalidades específicas ilustradas, mas, sim, ao âmbito de aplicação das reivindicações em apenso.

REIVINDICAÇÕES

1. Sistema para o monitoramento remoto de um dispositivo, compreendendo:

- pelo menos uma rede;

- pelo menos uma interface de rede no dispositivo associado à dita pelo menos uma rede;

- um agente host executável em um sistema operacional de host provido no dispositivo, o dito agente host sendo capaz de acessar a dita, pelo menos, uma rede através da dita, pelo menos, uma interface de rede;

- uma central de monitoramento conectada à dita, pelo menos, uma rede, configurada para se comunicar com pelo menos um dentre o agente host e um agente secundário através da dita, pelo menos, uma interface de rede; e

- um agente secundário provido no dispositivo, em que o agente secundário é capaz de acessar a dita, pelo menos, uma rede através da dita, pelo menos, uma interface de rede independentemente do sistema operacional host, e sendo que o agente secundário e o agente host coordenam quanto qual deverá acessar a dita pelo menos uma rede através da dita, pelo menos, uma interface de rede para comunicar os atributos do dispositivo e/ou do sistema operacional host para a central de monitoramento.

2. Sistema, de acordo com a reivindicação 1, no qual a dita, pelo menos, uma rede compreende uma primeira e segunda redes, em que a dita, pelo menos, uma interface de rede compreende uma interface de rede de host acessível tanto pelo agente host como pelo agente secundário para acessar a dita primeira rede, e uma interface de rede secundária à qual o agente secundário tem um acesso dedicado para se comunicar com a central de monitoramento através da segunda rede.

3. Sistema, de acordo com a reivindicação 2, no qual o agente secundário e a central de monitoramento se comunicam através da interface de rede secundária, quando a interface de rede host se torna indisponível.

4. Sistema, de acordo com a reivindicação 1, no qual o agente host é executado em um processador do dispositivo, e o agente secundário

é executado em um ambiente virtual no mesmo processador.

5. Sistema, de acordo com a reivindicação 1, no qual o agente host é executado em um processador do dispositivo, e o agente secundário é independentemente acionado de modo que possa funcionar independente do processador.

6. Sistema, de acordo com a reivindicação 5, no qual o agente secundário é configurado para continuar as operações do sistema operacional host a partir de um estado desativado.

7. Sistema, de acordo com a reivindicação 6, no qual o agente secundário contata a central de monitoramento e recebe instruções da central de monitoramento para continuar as operações do sistema operacional host, e solicitar o agente host para contatar a central de monitoramento.

8. Sistema, de acordo com a reivindicação 1, no qual o agente host e o agente secundário coordenam o acesso à dita pelo menos uma rede de forma a minimizar os encargos da rede.

9. Sistema, de acordo com a reivindicação 1, no qual o agente secundário acessa a dita, pelo menos, uma rede através da dita, pelo menos, uma interface de rede quando o agente host não é funcional para acessar a dita pelo menos uma rede.

10. Sistema, de acordo com a reivindicação 1, no qual o dispositivo é configurado para reinstalar o agente host quando o sistema operacional host detecta a presença do agente secundário.

11. Sistema, de acordo com a reivindicação 10, no qual o agente host provê um ou mais serviços de rastreamento e gerenciamento de dispositivos e, no qual as licenças associadas aos serviços são armazenadas em um local de armazenamento persistente no dispositivo.

12. Sistema, de acordo com a reivindicação 11, no qual após a instalação do sistema operacional, o agente host e o agente secundário são automaticamente instalados, e no qual, na ausência das licenças, o agente host e o agente secundário se desinstalam.

13. Sistema, de acordo com a reivindicação 1, no qual a dita, pelo menos, uma rede compreende uma rede celular.

14. Sistema, de acordo com a reivindicação 13, no qual a central de monitoramento solicita o agente host ou o agente secundário para contatar a central de monitoramento, através do envio de uma mensagem SMS para a rede celular.

15. Sistema, de acordo com a reivindicação 13, no qual a central de monitoramento é configurada para iniciar uma provisão de serviço na rede celular, no caso de uma provisão ser necessária antes de a utilização dos serviços de rede celular ser permitida.

16. Sistema, de acordo com a reivindicação 13, no qual o agente host ou o agente secundário contata a central de monitoramento através da rede celular, por meio do envio de uma mensagem SMS através de um modem de celular associado a um número, e no qual a central de monitoramento pode determinar o número das informações de origem contidas na mensagem SMS.

17. Sistema, de acordo com a reivindicação 1, no qual os serviços de rede na dita, pelo menos, uma rede são providos de modo a habilitar comunicações na dita, pelo menos, uma rede em resposta a um evento predeterminado que requer comunicação entre o dispositivo e a central de monitoramento.

18. Sistema, de acordo com a reivindicação 1, no qual a dita, pelo menos, uma interface de rede compreende pelo menos duas interfaces de rede, das quais uma é utilizada exclusivamente para comunicação com a central de monitoramento.

19. Sistema, de acordo com a reivindicação 1, no qual a dita, pelo menos, uma interface de rede compreende múltiplas interfaces de rede, e no qual o agente host e o agente secundário minimizam os encargos de rede ao selecionar o uso de redes de baixo custo.

20. Método de rastreamento de um dispositivo, compreendendo as etapas de:

- prover, pelo menos, uma interface de rede do dispositivo associado a pelo menos uma rede;

- prover um agente host executável em um sistema operacional

de host do dispositivo, o dito agente host sendo capaz de acessar a dita, pelo menos, uma rede através da dita, pelo menos, uma interface de rede;

- conectar uma central de monitoramento à dita, pelo menos, uma rede, configurada para se comunicar com pelo menos um agente host e um agente secundário através da dita, pelo menos, uma interface de rede;

- prover um agente secundário no dispositivo, capaz de acessar a dita, pelo menos, uma rede através da dita, pelo menos, uma interface de rede independentemente do sistema operacional host; e

- coordenar entre o agente secundário e o agente host a fim de determinar qual deverá acessar a dita, pelo menos, uma rede através da dita, pelo menos, uma interface de rede a fim de comunicar os atributos do dispositivo e/ou do sistema operacional host para a central de monitoramento.

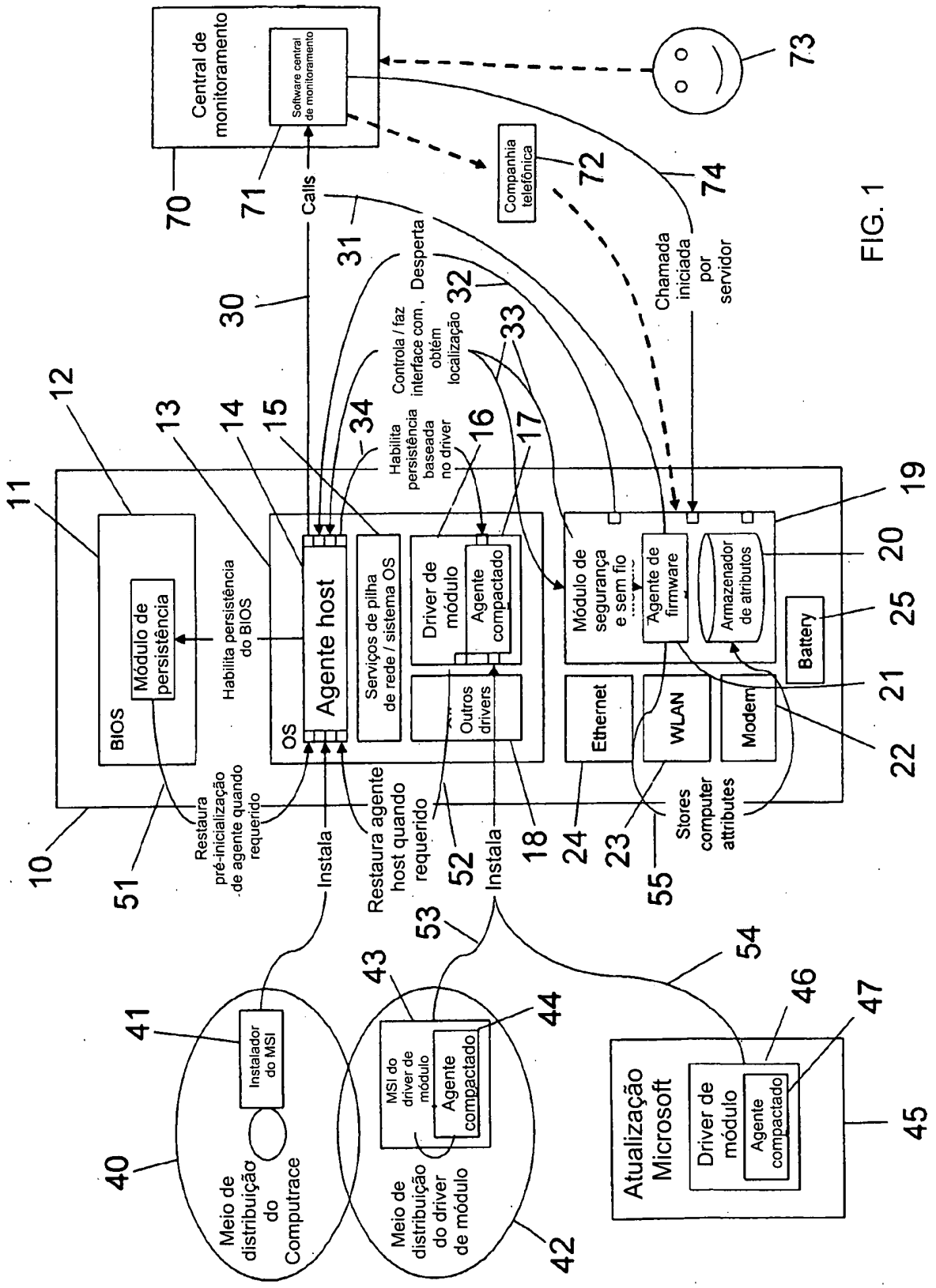

Central de monitoramento
Software central de monitoramento
70
71
Calls
73
Companhia telefônica
72
74
Chamada iniciada por servidor
Desperta
31
30
32
33
Controla / faz interface com , obtém localização
Habilita persistência baseada no driver
34
16
17
12
13
14
15
11
BIOS
Módulo de persistência
Habilita persistência do BIOS
OS
Agente host
Serviços de pilha de rede / sistema OS
Driver de módulo
Agente compactado
Outros drivers
Módulo de segurança e sem fio
Agente de firmware
Armazenador de atributos
Battery
Ethernet
WLAN
Modem
19
20
25
21
22
10
51
Restaura pré-inicialização de agente quando requerido
Instala
Restaura agente host quando requerido
52
Instala
18
24
23
55
Stores computer attributes
53
54
43
41
44
46
47
40
Instalador do MSI
MSI do driver de módulo
Agente compactado
Driver de módulo
Agente compactado
Atualização Microsoft
Meio de distribuição do Computrace
Meio de distribuição do driver de módulo
42
45

FIG. 1

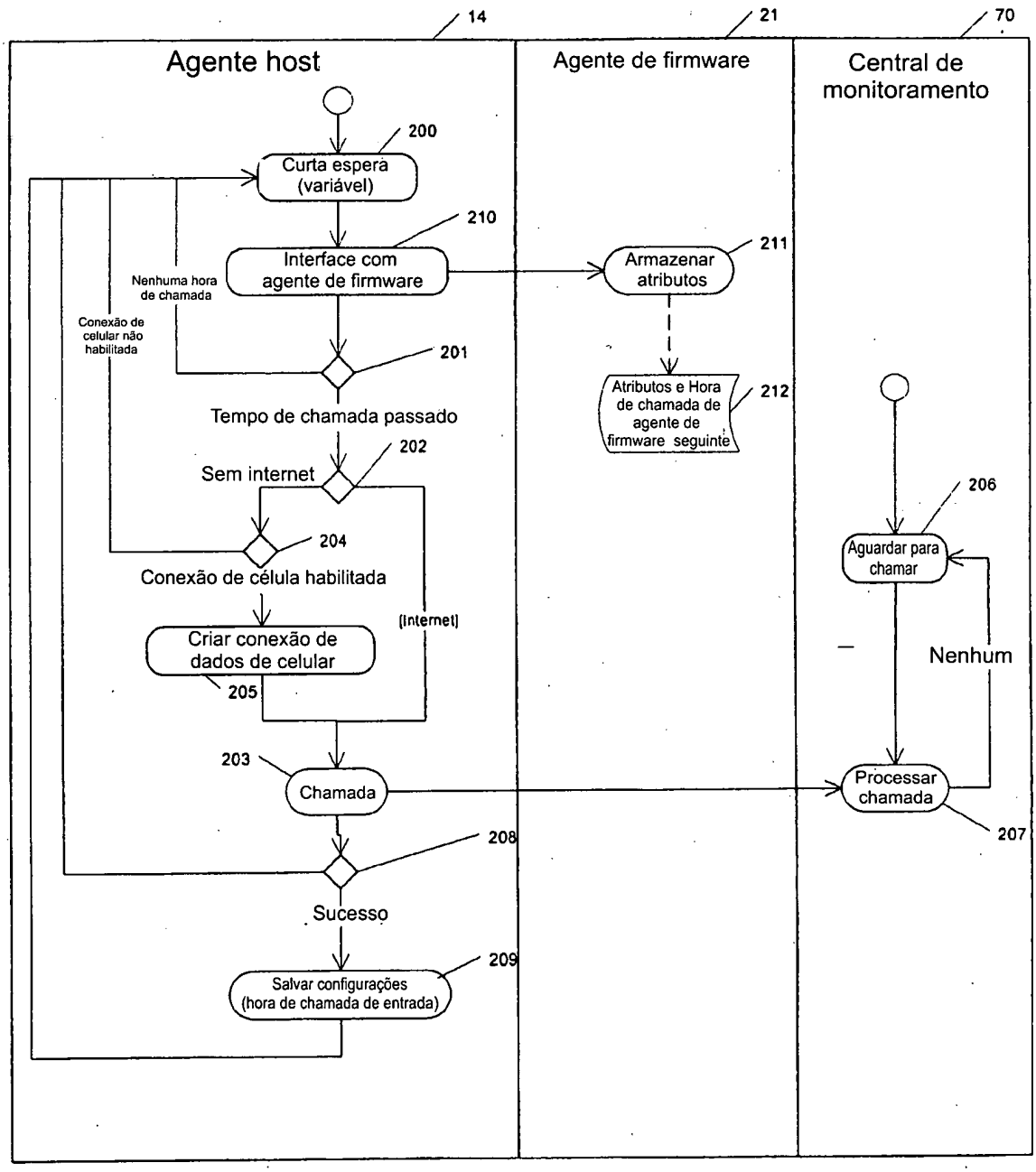

14
21
70
Agente host
Agente de firmware
Central de monitoramento
200
Curta espera (variável)
210
Interface com agente de firmware
211
Armazenar atributos
Nenhuma hora de chamada
Conexão de celular não habilitada
201
Atributos e Hora de chamada de agente de firmware seguinte
212
Tempo de chamada passado
202
Sem internet
206
204
Aguardar para chamar
Conexão de célula habilitada
[Internet]
Criar conexão de dados de celular
205
Nenhum
203
Chamada
Processar chamada
207
208
Sucesso
209
Salvar configurações (hora de chamada de entrada)

FIG. 2

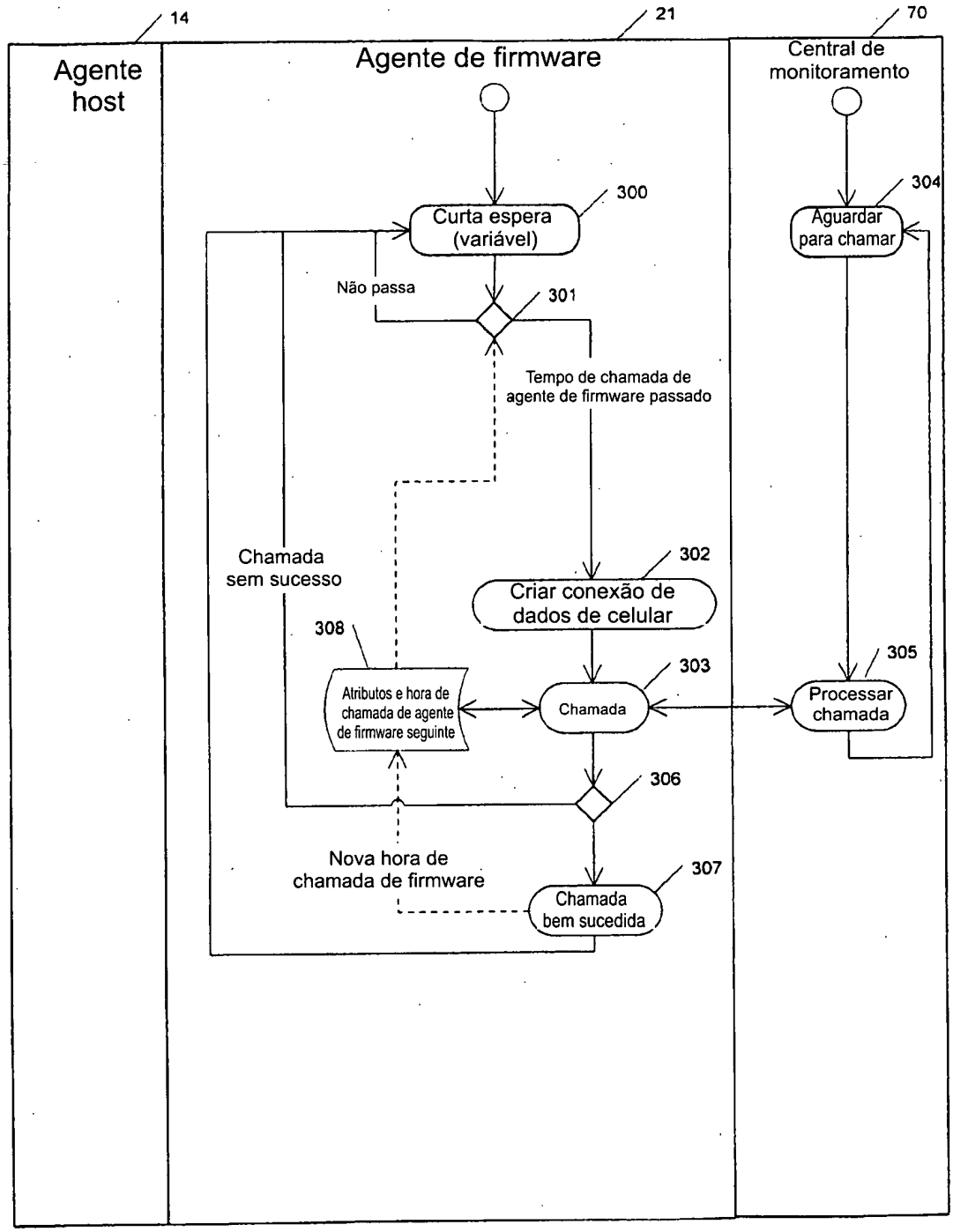

14
21
70
Agente host
Agente de firmware
Central de monitoramento
300
Curta espera (variável)
304
Aguardar para chamar
Não passa
301
Tempo de chamada de agente de firmware passado
Chamada sem sucesso
302
Criar conexão de dados de celular
308
305
Atributos e hora de chamada de agente de firmware seguinte
303
Chamada
Processar chamada
306
Nova hora de chamada de firmware
307
Chamada bem sucedida

FIG. 3

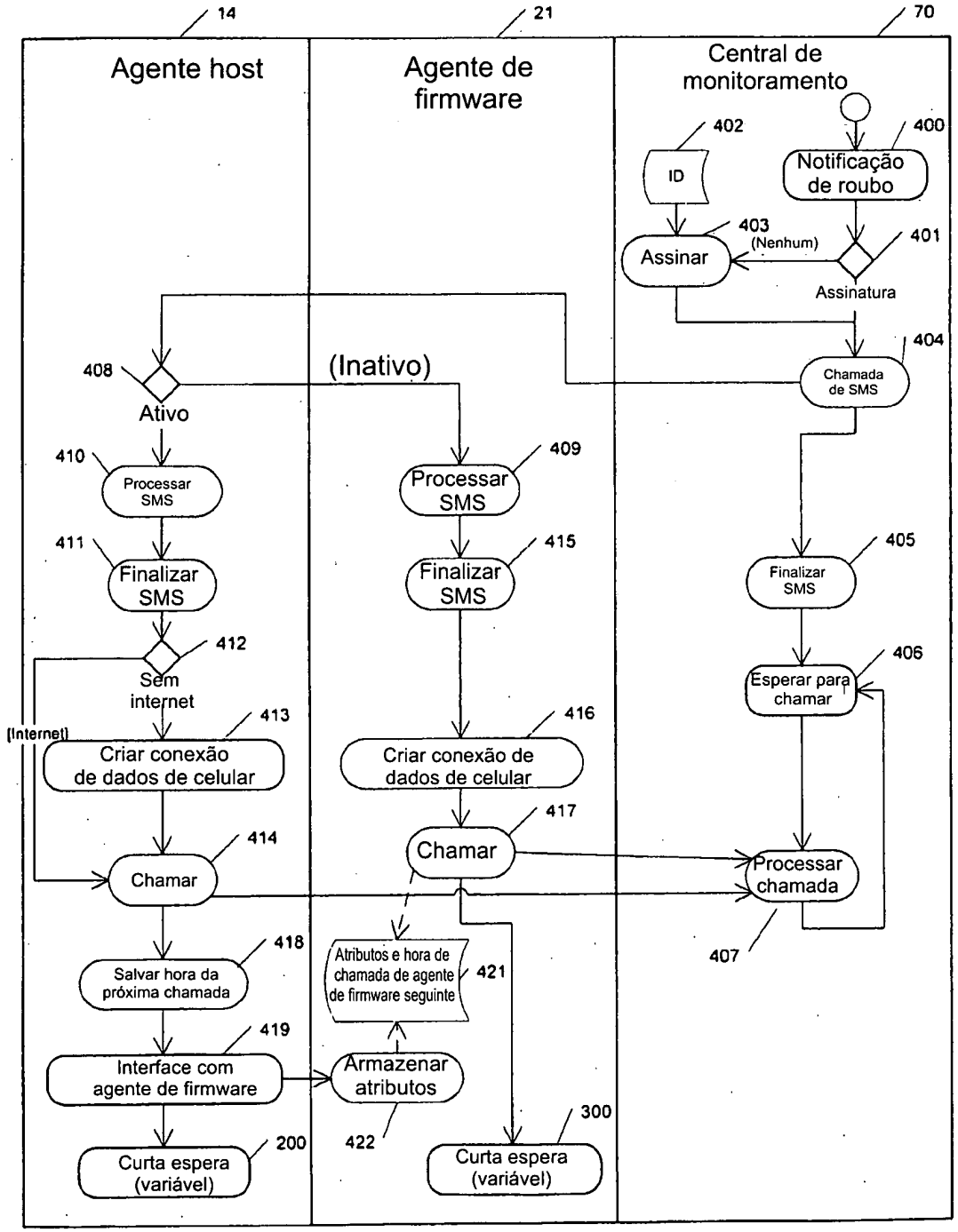

14
21
70
Agente host
Agente de firmware
Central de monitoramento
402
400
ID
Notificação de roubo
403
(Nenhum)
401
Assinar
Assinatura
404
408
(Inativo)
Chamada de SMS
Ativo
410
409
Processar SMS
Processar SMS
411
415
405
Finalizar SMS
Finalizar SMS
Finalizar SMS
412
406
Sem internet
Esperar para chamar
[Internet]
413
416
Criar conexão de dados de celular
Criar conexão de dados de celular
417
414
Chamar
Chamar
Processar chamada
418
421
407
Salvar hora da próxima chamada
Atributos e hora de chamada de agente de firmware seguinte
419
Interface com agente de firmware
Armazenar atributos
422
300
200
Curta espera (variável)
Curta espera (variável)

FIG. 4

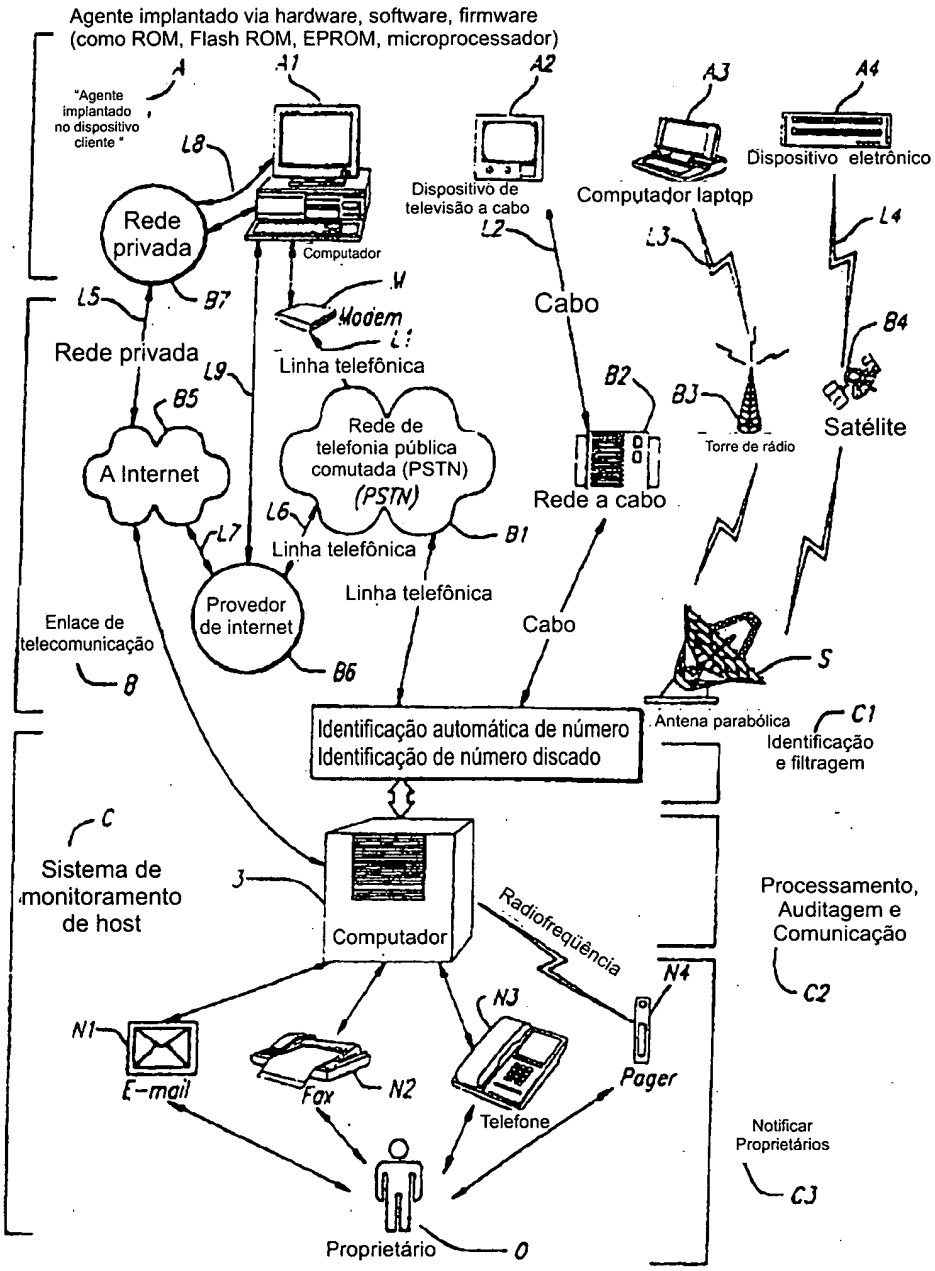

Agente implantado via hardware, software, firmware
(como ROM, Flash ROM, EPROM, microprocessador)
"Agente implantado no dispositivo cliente"
A
A1
A2
A3
A4
L8
Rede privada
Computador
Dispositivo de televisão a cabo
Computador laptop
Dispositivo eletrônico
L2
L3
L4
L5
B7
W
Modem
L1
Cabo
B4
Rede privada
Linha telefônica
L9
B2
B3
B5
Rede de telefonia pública comutada (PSTN)
(PSTN)
Torre de rádio
Satélite
A Internet
Rede a cabo
L6
L7
B1
Linha telefônica
Linha telefônica
Provedor de internet
Cabo
Enlace de telecomunicação
B
B6
S
Antena parabólica
C1
Identificação e filtragem
Identificação automática de número
Identificação de número discado
C
Sistema de monitoramento de host
J
Computador
Radiofreqüência
Processamento, Auditagem e Comunicação
C2
N1
N2
N3
N4
E-mail
Fax
Telefone
Pager
Notificar Proprietários
C3
Proprietário
O

FIG. 5

PI0806772-4

RESUMO

Patente de Invenção: **"MÓDULO DE SEGURANÇA TENDO UM AGENTE SECUNDÁRIO EM COORDENAÇÃO COM UM AGENTE HOST".**

A presente invenção refere-se a um módulo de segurança implantado em um dispositivo host, que provê um agente secundário que opera em coordenação com o agente host no dispositivo host, mas opera independente do sistema operacional de host do dispositivo host de modo a acessar independentemente uma interface de rede de comunicação existente no dispositivo host ou uma interface de rede dedicada separada, quando disponível. Em um aspecto, a presente invenção habilita serviços robustos de rastreamento de bens e recuperação de roubo. O sistema compreende uma central de monitoramento; um ou mais dispositivos monitorados; um módulo de segurança nos dispositivos monitorados; e uma ou mais redes de comunicação ativa. Os dispositivos monitorados podem ser dispositivos independentes, tais como computadores (por exemplo, computadores portáteis ou de mesa), ou um dispositivo ou um subsistema incluído em um sistema. Um dispositivo monitorado compreende um módulo de segurança, um agente host e um software para suportar o agente host executado no OS do dispositivo monitorado.