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

(21) **PI0615811-0 A2**

* B R P I 0 6 1 5 8 1 1 A 2 *

(22) Data de Depósito: 02/09/2006
(43) Data da Publicação: 24/05/2011
(RPI 2107)

(51) Int.Cl.:
G06F 15/78 2006.01
G06F 15/00 2006.01

(54) Título: **SISTEMA OPERACIONAL ENCERRADO EM UNIDADE DE PROCESSAMENTO**

(30) Prioridade Unionista: 12/09/2005 US 11/224.418

(73) Titular(es): MICROSOFT CORPORATION

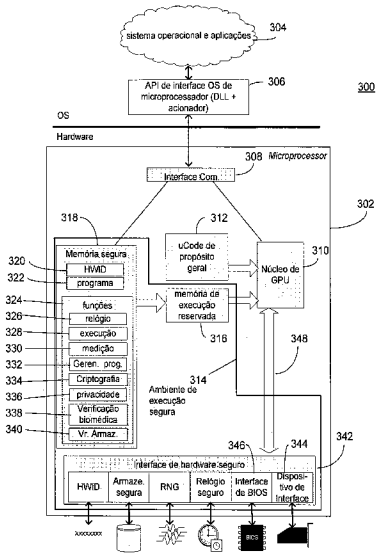
(72) Inventor(es): ALEXANDER FRANK, CURT A. STEEB, ISAAC P. AHDOUT, JAMES S. DUFFUS, MARTIN H. HALL, THOMAS PHILLIPS, ZHANGWEI XU

(74) Procurador(es): Alexandre Ferreira

(86) Pedido Internacional: PCT US2006034632 de 02/09/2006

(87) Publicação Internacional: WO 2007/032975de 22/03/2007

(57) Resumo: SISTEMA OPERACIONAL ENCERRADO EM UNIDADE DE PROCESSAMENTO. Uma unidade de processamento para uso em um dispositivo eletrônico inclui interfaces de comunicação e processamento de instrução padrão e também inclui capacidade funcional além de ou no lugar naquelas encontradas em um sistema operacional. Uma memória segura dentro da unidade de processamento pode conter um identificador de hardware, dados de programa, e funções de subsistema como um relógio seguro, gerencíamento de programa, e execução de programa. Os dados em funções dentro da memória de garantia não são acessíveis as partir do exterior da unidade de processamento.



"SISTEMA OPERACIONAL ENCERRADO EM UNIDADE DE PROCESSAMENTO"

ANTECEDENTES

Computadores que operam utilizando uma arquitetura com uma plataforma de processamento de hardware hospedando uma plataforma de operação de software, ou sistema operacional estão em uso. O sistema operacional é projetado para ser independente da plataforma de processamento (pelo menos em parâmetros amplos) e inversamente, a plataforma de processamento é projetada independentemente (nos mesmos parâmetros genericamente amplos) do sistema operacional. Por exemplo, Linux ou Microsoft Windows pode ser rodado na maioria das versões do processador Intel x86. Utilizando um monitor de máquina virtual (VMM) ou hipervisor, é possível rodar os dois sistemas operacionais simultaneamente. Similarmente, alguns sistemas operacionais, como UNIX, podem rodar em mais de um tipo de processador, por exemplo, processadores IBM PowerPC e Sun Sparc.

Essa independência entre plataforma de processamento e sistema operacional introduz riscos de segurança que podem ser explorados por pretensos hackers, em parte devido à dificuldade em estabelecer confiança entre o processador e o sistema operacional, isto é, entre o hardware e o software do computador. Os microprocessadores atuais entram em um ciclo "buscar e executar" que executa, de forma cega, as instruções dadas a ele e não estão preocupadas com o conteúdo ou ramificações das instruções executadas nem participam em decisões de programa relacionadas ao uso do dispositivo ele-

trônico.

SUMÁRIO

Uma unidade de processamento com funções de sistema incorporadas fornece uma base segura para executar programas de segurança e/ou operacionais, por exemplo, para uso na execução de operação pagar por uso, pay-as-you-go, ou outra operação medida de um dispositivo eletrônico como um computador, telefone celular, assistente pessoal digital, tocador de meios, etc. A unidade de processamento pode incluir recursos e suporte funcional encontrado na maioria ou em todos os microprocessadores modernos e também suportar funções adicionais que fornecem um identificador de hardware, um relógio resistente à violação e armazenagem segura. Outras capacidades funcionais como uma unidade criptográfica, podem estar presentes também. O resultado é uma unidade de processamento que não se baseia em quaisquer componentes externos, particularmente software de sistema operacional, um módulo de computação de confiança (TCM), ou BIOS de inicialização segura para estabelecer a base para computador capaz de ser operado em conformidade com um programa de uso.

Quando inicializada, a unidade de processamento determina qual programa está ativo e define a configuração do sistema de acordo com o programa, por exemplo, definir limites em memória disponível, número ou tipo de periféricos, ou comunicações de rede. O relógio provê um tempo confiável para uso em uso de medição, como uso durante um período de tempo, e como uma referência para detectar violação com o relógio do sistema.

BREVE DESCRIÇÃO DOS DESENHOS

A figura 1 é um diagrama de blocos representativo e simplificado de uma rede de computador;

A figura 2 é um diagrama de blocos de um computador que pode ser conectado à rede da figura 1;

A figura 3 é um diagrama de blocos de um computador mostrando detalhes da unidade de processamento; e

A figura 4 é um diagrama de blocos de um computador mostrando detalhes de uma modalidade alternativa da unidade de processamento da figura 3.

DESCRIÇÃO DETALHADA DE VÁRIAS MODALIDADES

Embora o texto a seguir exponha uma descrição detalhada de inúmeras modalidades diferentes, deve ser entendido que o escopo legal da descrição é definido pelas palavras das reivindicações expostas ao término dessa revelação. A descrição detalhada deve ser interpretada como exemplar somente e não descreve toda modalidade possível uma vez que a descrição de toda modalidade possível seria impraticável, se não impossível. Inúmeras modalidades alternativas poderiam ser implementadas, utilizando tecnologia atual ou tecnologia desenvolvida após a data de depósito dessa patente, que ainda estaria compreendida no escopo das reivindicações.

Deve ser também entendido que, a menos que um termo seja expressamente definido nessa patente utilizando a sentença "Como utilizado aqui, o termo "_____" é definido pela presente como significando..." ou uma sentença similar, não há intenção de limitar o significado daquele termo, expressamente ou por implicação, além de seu significado sim-

ples ou comum, e tal termo não deve ser interpretado como sendo limitado em escopo com base em qualquer declaração feita em qualquer seção dessa patente (diferente da linguagem das reivindicações). Até o ponto em que qualquer termo recitado nas reivindicações no final dessa patente seja mencionado nessa patente em um modo compatível com um significado único, isto é feito para fins de clareza somente de modo a não confundir o leitor, e não se pretende que esse termo de reivindicação seja limitado, por implicação ou de outro modo, àquele significado único. Finalmente, a menos que um elemento de reivindicação seja definido por recitar a palavra "significa" e uma função sem o recitall de qualquer estrutura, não se pretende que o escopo de qualquer elemento de reivindicação seja interpretado com base na aplicação de 35 U.S.C. § 112, sexto parágrafo.

Grande parte da funcionalidade inventiva e muitos dos princípios inventivos são melhores implementados com ou em programas de software ou instruções e circuitos integrados (ICs) como ICs de aplicação específica. Espera-se que uma pessoa com conhecimentos comuns, não obstante esforço possivelmente significativo e muitas escolhas de desenho motivadas, por exemplo, por tempo disponível, tecnologia atual, e considerações econômicas, quando guiada pelos conceitos e princípios revelados aqui seja prontamente capaz de gerar tais instruções e programas de software e ICs com experimentação mínima. Portanto, no interesse de brevidade e minimização de qualquer risco de obscurecer os princípios e conceitos de acordo com a presente invenção, discussão adi-

cional desse software e ICs, caso haja, será limitada ao essencial com relação aos princípios e conceitos das modalidades preferidas.

A figura 1 ilustra uma rede 10 que pode ser utilizada para implementar um sistema de computador de pagar por uso. A rede 10 pode ser a Internet, uma rede privada virtual (VPN), ou qualquer outra rede que permita que um ou mais computadores, dispositivos de comunicação, bancos de dados, etc., sejam conectados de forma comunicativa entre si. A rede 10 pode ser conectada a um computador pessoal 12 e um terminal de computador 14 através de um Ethernet 16 e um roteador 18, e uma linha física 20. Por outro lado, a rede 10 pode ser conectada sem fio a um computador laptop 22 e um assistente pessoal de dados 24 através de uma estação de comunicação sem fio 26 e uma ligação sem fio 28. Similarmente, um servidor 30 pode ser conectado à rede 10 utilizando uma ligação de comunicação 32 e um mainframe 34 pode ser conectado à rede 10 utilizando outra ligação de comunicação 36.

A figura 2 ilustra um dispositivo de computação na forma de um computador 110 que pode ser conectado à rede 10 e utilizado para implementar um ou mais componentes do sistema de provisionamento de software dinâmico. Os componentes do computador 110 podem incluir, porém não são limitados a, uma unidade de processamento 120, uma memória de sistema 130, e um barramento de sistema 121 que acopla vários componentes de sistema incluindo a memória de sistema 130 à unidade de processamento 120. O barramento de sistema 121 pode ser qualquer de vários tipos de estruturas de barramento in-

cluindo um barramento de memória ou controlador de memória, um barramento periférico, e um barramento local utilizando qualquer de uma variedade de arquiteturas de barramento. Como exemplo, e não limitação, essas arquiteturas incluem barramento de Industry Standard Architecture (ISA), barramento de Micro Channel Architecture (MCA), barramento de ISA aperfeiçoado (EISA), barramento local de Video Electronics Standards Association (VESA) e barramento de Peripheral Component Interconnect (PCI) também conhecido como barramento Mezzanine.

A unidade de processamento 120 pode ser um microprocessador como um microprocessador disponível junto a Intel, ou outros, como é sabido na técnica. A unidade de processamento pode ser um chip único ou pode ser uma unidade de processador múltiplo e pode incluir chips periféricos associados (não representados) ou blocos funcionais (não representados). Tais chips associados podem incluir pré-processadores, chips de pipeline, memórias intermediárias simples e acionadores, ou podem incluir conjuntos de chip/chip mais complexos como os chips "Northbridge" e "Southbridge" conhecidos em algumas arquiteturas de computador de tecnologia atual. A unidade de processamento 120 também pode incluir um ambiente de execução segura 125, no mesmo silício que o microprocessador ou como um chip relacionado como parte da unidade de processamento geral. O ambiente de execução segura 125 e sua interação com a unidade de processamento, ou dispositivos equivalentes, é discutido em mais detalhe abaixo com relação à figura 3 e a figura 4.

O computador 110 inclui, tipicamente, uma variedade de meios legíveis por computador. Os meios legíveis por computador podem ser quaisquer meios disponíveis que podem ser acessados pelo computador 110 e incluem tanto meios voláteis como não voláteis, meios removíveis e não removíveis. Como exemplo, e não limitação, meios legíveis por computador podem compreender meios de armazenagem em computador e meios de comunicação. Os meios de armazenagem de computador incluem meios voláteis e não voláteis, removíveis e não removíveis implementados em qualquer método ou tecnologia para armazenagem de informações como instruções legíveis por computador, estruturas de dados, módulos de programa ou outros dados. Meios de armazenagem de computador incluem, porém não são limitados a, RAM, ROM, EEPROM, memória flash ou outra tecnologia de memória, CD-ROM, digital versatile disks (DVD) ou outra armazenagem de disco óptico, cassetes magnéticos, fita cassete, armazenagem de disco magnético ou outros dispositivos de armazenagem magnética, ou qualquer outro meio que pode ser utilizado para armazenar as informações desejadas e que pode ser acessado por computador 110. Os meios de comunicação incorporam, tipicamente, instruções legíveis por computador, estruturas de dados, módulos de programa ou outros dados em um sinal de dados modulado como uma onda portadora ou outro mecanismo de transporte e inclui qualquer meio de fornecimento de informações. O termo "sinal de dados modulado" significa um sinal que tem uma ou mais de suas características definidas ou alteradas de tal modo a codificar informações no sinal. Como exemplo, e não limitação, meios

de comunicação incluem meios cabeados como uma rede cabeada ou conexão cabeada direta, e meios sem fio como meios acústicos, e radiofreqüência, infravermelho e outros meios sem fio. As combinações de qualquer um dos acima também devem ser incluídas no escopo dos meios legíveis por computador.

A memória do sistema 130 inclui meios de armazenagem de computador na forma de memória volátil e/ou não volátil como memória somente de leitura (ROM) 131 e memória de acesso aleatório (RAM) 132. Um sistema de entrada/saída básico 133 (BIOS), contendo as rotinas básicas que ajudam a transferir informações entre elementos no computador 110, como durante partida, é tipicamente armazenado na ROM 131. A RAM 132 contém, tipicamente, dados e/ou módulos de programa que são imediatamente acessíveis a e/ou sendo atualmente operados pela unidade de processamento 120. Como exemplo, e não limitação, a figura 2 ilustra o sistema operacional 134, programas de aplicação 135, outros módulos de programa 136, e dados de programa 137.

O computador 110 também pode incluir outros meios de armazenagem de computador removíveis/não removíveis, voláteis/não voláteis. Somente como exemplo, a figura 2 ilustra uma unidade de disco rígido 140 que lê de ou grava para meios magnéticos não removíveis, não voláteis, uma unidade de disco magnético 151 que lê de ou grava para um disco magnético removível, não volátil 152, e uma unidade de disco óptico 155 que lê de ou grava para um disco óptico removível, não volátil 156 como um RD COM ou outro meio óptico. Outros meios de armazenagem de computador removíveis/não re-

movíveis, voláteis/não voláteis que podem ser utilizados no ambiente operacional exemplar incluem, porém não são limitados a, cassetes de fita magnética, cartões de memória flash, digital versatile disks, fita de vídeo digital, RAM de estado sólido, ROM de estado sólido, e similares. A unidade de disco rígido 141 é tipicamente conectada ao barramento de sistema 121 através de uma interface de memória não removível como interface 140, e unidade de disco magnético 151 e unidade de disco óptico 155 são tipicamente conectadas ao barramento de sistema 121 por uma interface de memória removível, como interface 150.

As unidades e seus meios de armazenagem de computador associados discutidos acima e ilustrados na figura 2, fornecem armazenagem de instruções legíveis por computador, estruturas de dados, módulos de programa e outros dados para o computador 110. Na figura 2, por exemplo, a unidade de disco rígido 141 é ilustrada como armazenando o sistema operacional 144, programas de aplicação 145, outros módulos de programa 146, e dados de programa 147. Observe que esses componentes podem ser iguais a ou diferentes ao sistema operacional 134, programas de aplicação 135, outros módulos de programa 136, e dados de programa 137. O sistema operacional 144, programas de aplicação 145, outros módulos de programa 146, e dados de programa 147 recebem números diferentes aqui para ilustrar que, no mínimo, são cópias diferentes. Um usuário pode entrar comandos e informações no computador 20 através de dispositivos de entrada como teclado 162 e dispositivo de indicação 161, comumente mencionado como um mouse,

TrackBall ou touch pad. Outro dispositivo de entrada pode ser uma câmera para enviar imagens através da Internet, conhecida como uma web cam 163. Outros dispositivos de entrada (não mostrados) podem incluir um microfone, manche, game pad, prato de satélite, scanner, ou similar. Esses e outros dispositivos de entrada são freqüentemente conectados à unidade de processamento 120 através de uma interface de entrada de usuário 160 que é acoplada ao barramento de sistema, porém podem ser conectados por outras estruturas de barramento e interface, como porta paralela, porta de jogo ou um barramento serial universal (USB). Um monitor 191 ou outros tipos de dispositivo de exibição também é conectado ao barramento do sistema 121 através de uma interface, como uma interface de vídeo 190. Além do monitor, computadores também podem incluir outros dispositivos de saída periféricos como alto-falantes 197 e impressora 196, que podem ser conectados através de uma interface periférica de saída 195.

O computador 110 pode operar em um ambiente ligado em rede utilizando conexões lógicas a um ou mais computadores remotos, como um computador remoto 180. O computador remoto 180 pode ser um computador pessoal, um servidor, um roteador, um PC de rede, um dispositivo par ou outro nó de rede comum, e tipicamente inclui muitos ou todos os elementos descritos acima em relação ao computador 110, embora somente um dispositivo de armazenagem de memória 181 tenha sido ilustrado na figura 2. As conexões lógicas representadas na figura 2 incluem uma rede de área local (LAN) 171 e uma rede remota (WAN) 173, porém também podem incluir outras redes.

Tais ambientes de ligação em rede são comuns em escritórios, redes de computador de empresas, intranets, e Internet.

Quando utilizado em um ambiente de ligação em rede LAN, o computador 100 é conectado à LAN 171 através de uma interface de rede ou adaptador 170. Quando utilizado em um ambiente de ligação em rede WAN, o computador 100 inclui tipicamente um modem 172 ou outro meio para estabelecer comunicação através da WAN 173, como Internet. O modem 172, que pode ser interno ou externo, pode ser conectado ao barramento de sistema 121 através da interface de entrada de usuário 160, ou outro mecanismo apropriado. Em um ambiente ligado em rede, módulos de programa representados em relação ao computador 100, ou porções do mesmo, podem ser armazenados no dispositivo de armazenagem de memória remoto. Como exemplo, e não limitação, a figura 2 ilustra programas de aplicação remota 185 como residindo no dispositivo de memória 181. Será reconhecido que as conexões de rede mostradas são exemplos e outros meios de estabelecer uma ligação de comunicação entre os computadores podem ser utilizados.

A figura 3 representa um diagrama de blocos simplificado de um computador 300. O computador inclui uma unidade de processamento 302, que pode ser similar a ou igual à unidade de processamento 120. O diagrama de blocos também representa o computador 300 tendo um sistema operacional e aplicações 304 que são acoplados à unidade de processamento 302 por uma interface de programa de aplicação de interface (API) 306. A API 306 pode comunicar-se com uma interface de comunicação 308 na unidade de processamento 302. A interface

de comunicação 308 pode ter a forma de um handler de interrupção ou handler de processamento de mensagem, unidade de análise, etc. Como encontrado em microprocessadores convencionais, a unidade de processamento 302 pode incluir um núcleo de unidade de processamento geral (GPU) 310 que processa instruções de propósito geral recebidas através da interface de comunicação 308 utilizando um conjunto de microcódigo de propósito geral 312. A operação do núcleo de GPU 310 e sua relação com o microcódigo de propósito geral 312 é bem documentado e entendido na indústria, e é exemplificado em processadores como a série Intel Pentium™, processadores ARM™ a partir de Advanced Rise Machines Limited, e processador PowerPC™ da IBM.

Um ambiente de execução segura 314 pode suplementar as capacidades de processamento geral fornecidas pelo núcleo de GPU e microcódigo 310 312. O ambiente de execução segura 314 pode incluir uma memória de execução reservada 316. A memória de execução reservada 316 pode fornecer um local altamente seguro para a execução de instruções tendo um nível de privilégio elevado dentro da unidade de processamento 302. Esse nível de operação de privilégio elevado pode permitir que a unidade de processamento 302 execute código que não é diretamente acessível a partir do exterior da unidade de processamento 302. Por exemplo, um vetor de interrupção específico pode definir a unidade de processamento 302 em operação segura, ou instruções podem ser avaliadas em relação a conteúdo exigindo recursos seguros. Ao operar nesse modo de privilégio elevado, a unidade de processamento

302 atua como um subsistema completo e não requer nenhum bem ativo, por exemplo recursos de BIOS, memória de programa, ou um TCM, para construir um ambiente de processamento seguro.

Uma memória segura 318 pode armazenar, em um modo resistente à violação, código e dados relacionados à operação segura do computador 302. A interface de comunicação 308 pode determinar quais instruções que entram no processador 302 devem ser dirigidas à memória segura 318, e subseqüentemente para execução na memória de execução reservada 316. Os dados na memória segura 318 podem incluir um sinal de identificação ou identificador de hardware 320 e dados de programa 322 que podem especificar diretivas operacionais relacionadas ao programa como medição, reportar, exigências de atualização, etc. A memória segura 318 pode incluir também código ou dados necessários para implementar várias funções 324. As funções 324 podem incluir um relógio 326 ou temporizador implementando funções de relógio, funções de execução 328, medição 330, gerenciamento de programa 332, criptografia 334, privacidade 336, verificação biométrica 338, e valor armazenado 340 citando alguns.

O relógio 326 pode fornecer uma base segura para medição de tempo e pode ser utilizado como uma verificação contra um relógio de sistema mantido pelo sistema operacional 134 para ajudar a evitar tentativas de uso fraudulento do computador 300 pela alteração do relógio do sistema. O relógio 326 pode ser utilizado também em combinação com o gerenciamento do programa 332, por exemplo, para exigir comunicação com um servidor hospedeiro para verificar a dispo-

nibilidade de upgrade. As funções de execução 328 podem ser carregadas na memória de execução reservada 316 e executadas quando for determinado que o computador 300 não está em conformidade com um ou mais elementos do programa 322. Tais ações podem incluir restrição da memória do sistema 132 pela orientação da unidade de processamento 302 para alocar memória de sistema genericamente disponível para uso pelo ambiente de execução segura 314. Pela realocação da memória do sistema 134 para o ambiente de execução segura 314, a memória do sistema 134 é essencialmente tornada indisponível para finalidades do usuário.

Outra função 324 pode ser medição 330. Medição 330 pode incluir uma variedade de técnicas e medições, por exemplo, aquelas como discutido no pedido de patente US copendente número de série 11/006.837. O fato de se deve medir e quais itens específicos medir pode ser uma função do programa 322 é implementado pela função de gerenciamento do programa 332. Uma função de criptografia 334 pode ser utilizada para verificação de assinatura digital, assinatura digital, geração de número aleatório, e criptografia/decriptografia. Qualquer uma ou todas essas capacidades podem ser utilizadas para verificar atualizações na memória segura 318 ou confiança estabelecida com uma entidade fora da unidade de processamento 302 quer dentro ou fora do computador 300.

O ambiente de execução segura 314 pode permitir que várias funções de propósito especial sejam desenvolvidas e utilizadas. Um gerenciador de privacidade 336 pode ser utilizado para gerenciar informações pessoais para um usuário

ou parte interessada. Por exemplo, o gerenciador de privacidade 336 pode ser utilizado para implementar uma função de "carteira" para reter dados de cartão de crédito e endereço para uso em compras on-line. Uma função de verificação biométrica 338 pode ser utilizada com um sensor biométrico externo para verificar identidade pessoal. Tal verificação de identidade pode ser utilizada, por exemplo, para atualizar informações pessoais no gerenciador de privacidade 336 ou ao aplicar uma assinatura digital. Como mencionado acima, a função de criptografia 334 pode ser utilizada para estabelecer confiança e um canal seguro para um sensor biométrico externo (não representado).

Uma função de valor armazenado 340 pode ser implementada também para uso no pagamento por tempo em um computador de pagar por uso ou enquanto faz uma compra externa, por exemplo, transações de comércio de ações on-line.

O uso de dados e funções a partir da memória segura 318 para execução na memória de execução reservada 316 permite apresentação de uma interface de hardware segura 342. A interface de hardware segura 342 permite acesso restrito e ou monitorado a dispositivos periféricos 344 ou BIOS 346. Adicionalmente as funções 324 podem ser utilizadas para permitir que programas externos, incluindo o sistema operacional 134, acessem instalações seguras como ID de hardware e geração de número aleatório através de conexão lógica 348 entre a GPU 310 na interface de hardware segura 342. Além disso, cada função discutida acima, como implementado em código e armazenado na memória segura 318 pode ser implementa-

da em lógica e instanciada como um circuito físico. As operações para mapear comportamento funcional entre hardware e software são bem conhecidas na técnica e não são discutidas aqui em mais detalhe.

Em operação, uma interrupção designada pode ser processada pela interface de comunicação 308 fazendo com que dados ou uma ou mais funções sejam carregadas a partir da memória segura 318 na memória de execução reservada 316. A GPU 310 pode executar a partir da memória de execução reservada 316 para implementar a função. Em uma modalidade, as funções 324 disponíveis podem suplementar ou substituir funções padrão disponíveis no sistema operacional 134. Quando configurado desse modo, um sistema operacional correspondente 134 operará somente quando emparelhado com a unidade de processamento 302. Levando esse conceito para outro nível, outra modalidade da unidade de processamento 302 pode ser programada para reter funções do sistema operacional externo a menos que executadas a partir da memória de execução reservada 316. Por exemplo, tentativas em alocar memória pelo sistema operacional externo 134 podem ser negadas ou redirecionadas para funções internamente armazenadas. Quando configurado desse modo, somente um sistema operacional especificamente configurado para a unidade de processamento 302 operará corretamente. Ainda em outra modalidade, dados de programa 322 e funções de gerenciamento de programa 332 podem testar sistema operacional 134, programa de aplicação 135, e parâmetros de hardware para assegurar que software e hardware autorizados estejam presentes.

Em uma modalidade, o computador 300 inicializa utilizando um procedimento de partida BIOS normal. Em um ponto quando o sistema operacional 134 está sendo ativado, a unidade de processamento 302 pode carregar a função de gerenciamento de programa 332 na memória de execução reservada 316 para execução para configurar o computador 300 de acordo com os dados do programa 322. O processo de configuração pode incluir alocação de memória, capacidade de processamento, disponibilidade periférica e uso bem como exigências de medição. Quando medição deve ser executada, os programas referentes à medição, como quais medições fazer, por exemplo, pelo uso de CPU ou durante um período de tempo, podem ser ativados. Adicionalmente, quando o uso é carregado por período ou por atividade, um resto de valor armazenado pode ser mantido utilizando a função de valor armazenado 340. Quando o computador 300 foi configurado de acordo com o programa 322, o processo de inicialização normal pode continuar pela ativação e instanciação do sistema operacional 134 e outros programas de aplicação 135. Em outras modalidades, o programa pode ser aplicado em pontos diferentes no processo de inicialização ou ciclo de operação normal.

Caso não conformidade com o programa seja descoberta, a função de execução 328 pode ser ativada. Uma discussão de programa de execução e ações pode ser encontrada no pedido copendente Pedido de patente Norte-americana número de série: 11/152.214. A função de execução 328 pode colocar o computador 300 em um modo de operação alternativo quando todas as tentativas em retornar o computador para

conformidade com o programa 322, falham. Por exemplo, em uma modalidade, uma sanção pode ser imposta por realocar a memória a partir de uso como memória de sistema 130 e designar a mesma como memória segura 318. Uma vez que a memória segura 318 não é endereçável por programas externos incluindo o sistema operacional 134, a operação do computador pode ser restrita, mesmo severamente, por essa alocação de memória.

Como as funções de execução e programa são mantidas na unidade de processamento 302, alguns ataques típicos no sistema são difíceis ou impossíveis. Por exemplo, o programa não pode ser "dissimulado" pela substituição de uma seção de memória de programa de memória externa. Similarmente, as funções de execução e programa não podem ficar "em falta" pelo bloqueio de ciclos de execução e suas respectivas faixas de endereço.

Para reverter o computador 300 para operação normal, um código de recuperação pode necessitar ser adquirido a partir de uma autoridade de licenciar ou provedor de serviço (não representado) e entrado no computador 300. O código de recuperação pode incluir a ID de hardware 320, um reabastecimento de valor armazenado, e um tempo "não mais cedo do que" utilizado para verificar o relógio 326. O código de recuperação pode ser tipicamente criptografado e assinado para confirmação pela unidade de processamento 302.

Atualizações adicionais nos dados na memória segura 318 podem ser permitidas somente quando critérios específicos são atendidos, por exemplo, quando as atualizações são verificadas por assinatura digital.

A figura 4 é um diagrama de blocos de um computador 400 mostrando uma modalidade alternativa da unidade de processamento 302 mostrada na figura 3. O computador 400 tem uma unidade de processamento 402, um sistema operacional 404 e uma interface de programa de aplicação (API) da interface de sistema operacional de microprocessador, 406. A unidade de processamento 402 inclui uma interface de comunicação 408 que pode operar em um modo similar à interface de comunicação 308 pela orientação de tráfego de dados para uma função de microprocessador apropriada baseada em um critério como características de interrupção ou faixa de endereço. A unidade de processamento 402 pode ter uma unidade de processamento geral convencional (GPU) 410 e microcódigo de propósito geral correspondente, 412. Um ambiente de execução segura 414 pode incluir funções iguais ou similares encontradas no ambiente de execução segura 314 com a adição de um processador de núcleo seguro separado, 416. O processador de núcleo seguro 416 pode permitir um nível adicional de independência a partir do núcleo de GPU 410 e um aumento correspondente na garantia da unidade de processamento 402.

A memória segura 418 pode incluir uma ID de hardware 420 e dados de programa 422 além das funções de propósito geral 424 que operam como discutido acima, com relação à figura 3, por exemplo relógio 426, execução 428, medição 430, gerenciamento de programa 432, e criptografia 434. Adicionalmente, as funções de propósito especial como gerenciamento de privacidade 436, verificação biométrica 438, e valor armazenado 440 podem estar presentes. As funções de pro-

pósito geral e propósito especial 424 são dadas como exemplo e não limitação, visto que outras funções são facilmente imaginadas por aqueles com conhecimentos comuns na técnica.

A apresentação de dispositivos à interface de hardware segura 442, como uma interface de dispositivo 444 e a interface de BIOS 446, bem como a apresentação de funções como um relógio seguro e gerador de número aleatório pode ser feita através de conexão virtual 448. A comunicação entre o núcleo de GPU 410 no processador de núcleo seguro 416 pode ser feita através de um barramento de comunicação 450. Em uma modalidade, o barramento de comunicação 450 pode transmitir dados através de um canal seguro para estender a relação de confiança a partir do processador de núcleo seguro 416 com a GPU 410.

São descritas acima várias modalidades específicas incluindo modalidades de hardware e software para medição delicada de uso de computador. Um método mais razoável e preciso de determinar e medir uso benéfico é revelado por monitorar e avaliar níveis de atividade de um ou mais componentes do computador 110 e aplicar regras comerciais apropriadas. Isso beneficia uma faixa ampla de aplicações de pagar por uso ou uso medido domésticas, de escritório e empresa. Entretanto, uma pessoa com conhecimentos comuns na técnica reconhecerá que várias modificações e alterações podem ser feitas nessas modalidades, incluindo ´porém não limitadas ao uso de diferentes combinações de hardware ou software para monitoração de atividade, múltiplos programas de taxas, bem como regras mais ou menos complexas associadas à deter-

minação de um programa de uso apropriado. Por conseguinte, o relatório descritivo e desenhos devem ser considerados em um sentido ilustrativo em vez de restritivo, e todas essas modificações pretendem estar incluídas no escopo da presente patente.

REIVINDICAÇÕES

1. Unidade de processamento para uso em um dispositivo eletrônico, **CARACTERIZADA** por compreender:

uma unidade de processamento de instrução;

uma interface de comunicação;

um sinal de identificação;

um circuito de gerenciamento de programa;

um circuito de execução;

um circuito de relógio que fornece uma base de tempo que aumenta de forma monotônica; e

uma memória resistente à violação que armazena dados correspondendo a um programa de uso que regula operação do dispositivo eletrônico em conformidade com o programa de uso.

2. Unidade de processamento, de acordo com a reivindicação 1, **CARACTERIZADA** pelo fato de que o programa de uso especifica uma definição de sistema correspondendo a uso de recurso no dispositivo eletrônico.

3. Unidade de processamento, de acordo com a reivindicação 1, **CARACTERIZADA** pelo fato de que o programa de uso compreende um valor operacional que corresponde a pelo menos uma medição por tempo e medição por uso.

4. Unidade de processamento, de acordo com a reivindicação 1, **CARACTERIZADA** por compreender ainda código de software armazenado na memória resistente à violação implementando uma função de privacidade, a função de privacidade para garantir informações correspondendo aos dados de usuário.

5. Unidade de processamento, de acordo com a reivindicação 1, **CARACTERIZADA** pelo fato de que a interface de comunicação provê dados para uma interface de programa de aplicação para comunicar atualizações de programa.

6. Unidade de processamento, de acordo com a reivindicação 1, **CARACTERIZADA** pelo fato de que o circuito de gerenciamento de programa determina quando medir uso do dispositivo eletrônico.

7. Unidade de processamento, de acordo com a reivindicação 1, **CARACTERIZADA** pelo fato de que o circuito de execução limita a operação do dispositivo eletrônico quando o circuito de gerenciamento de programa determina que a operação não está em conformidade com o programa.

8. Unidade de processamento, de acordo com a reivindicação 1, **CARACTERIZADA** por compreender ainda código de software armazenado na memória resistente à violação para implementar uma função de autenticação de biométrica.

9. Unidade de processamento, de acordo com a reivindicação 1, **CARACTERIZADA** por compreender ainda código de software armazenado na memória resistente à violação para implementar uma função criptográfica, pelo que uma atualização de programa é verificada de forma criptográfica antes da instalação.

10. Unidade de processamento, de acordo com a reivindicação 9, **CARACTERIZADA** pelo fato de que a função criptográfica é operável para estabelecer uma relação de confiança com outro componente do dispositivo eletrônico.

11. Unidade de processamento, de acordo com a rei-

vindicação 1, **CARACTERIZADA** pelo fato de que o programa define uma configuração de hardware.

12. Unidade de processamento, de acordo com a reivindicação 1,. **CARACTERIZADA** pelo fato de que o programa define uma configuração de memória que exclui memória de sistema externo a partir do uso geral por alocação da memória de sistema externo à memória resistente à violação.

13. Unidade de processamento, de acordo com a reivindicação 1, **CARACTERIZADA** por compreender ainda código de software armazenado na memória resistente à violação para implementar uma função de valor armazenado.

14. Computador adaptado para uso em conformidade com um programa que corresponde a pelo menos um entre uma configuração de memória, uma capacidade de processamento, uma exigência de medição, e autorização para um periférico, o computador sendo **CARACTERIZADO** por compreender:

uma memória volátil;

uma memória não volátil;

uma interface de entrada;

uma interface de comunicação; e

uma unidade de processamento acoplada à memória volátil, memória não volátil, interface de entrada, e interface de saída, a unidade de processamento compreendendo:

uma unidade de processamento de instrução;

uma interface de barramento de dados;

uma função de gerenciamento de programa;

uma função de execução;

um relógio resistente à violação; e

uma memória segura que armazena o programa;

em que o computador opera de acordo com o programa armazenado na memória segura.

15. Computador, de acordo com a reivindicação 14, **CARACTERIZADO** pelo fato de que os dados correspondendo ao programa são recebidos através de uma entre a interface de entrada e a interface de comunicação.

16. Computador, de acordo com a reivindicação 14, **CARACTERIZADO** pelo fato de que a unidade de processamento compreende ainda uma função criptográfica.

17. Método de operar um computador tendo uma unidade de processamento com uma memória resistente à violação, o método sendo **CARACTERIZADO** por compreender:

executar instruções de computador para inicializar o computador;

executar instruções de computador para ler um programa a partir da memória resistente à violação, o programa correspondendo pelo menos a uma configuração de memória, uma capacidade de processamento, uma exigência de medição, e autorização para um periférico; e

executar instruções de computador para operar o computador de acordo com o programa.

18. Método, de acordo com a reivindicação 17, **CARACTERIZADO** por compreender ainda:

colocar o computador em um modo de uso restrito;

receber um código de recuperação incluindo uma indicação de tempo; e

comparar a indicação de tempo com uma função in-

terna de relógio.

19. Método, de acordo com a reivindicação 17, **CARACTERIZADO** por compreender ainda:

determinar quando o programa requer uso medido do computador;

medir o uso de acordo com o programa.

20. Método, de acordo com a reivindicação 17, **CARACTERIZADO** pelo fato de que executar instruções de computador para operar o computador de acordo com o programa, compreende ainda executar instruções de computador para realocar memória de sistema para a memória resistente à violação tornando a mesma indisponível para uso geral pelo computador.

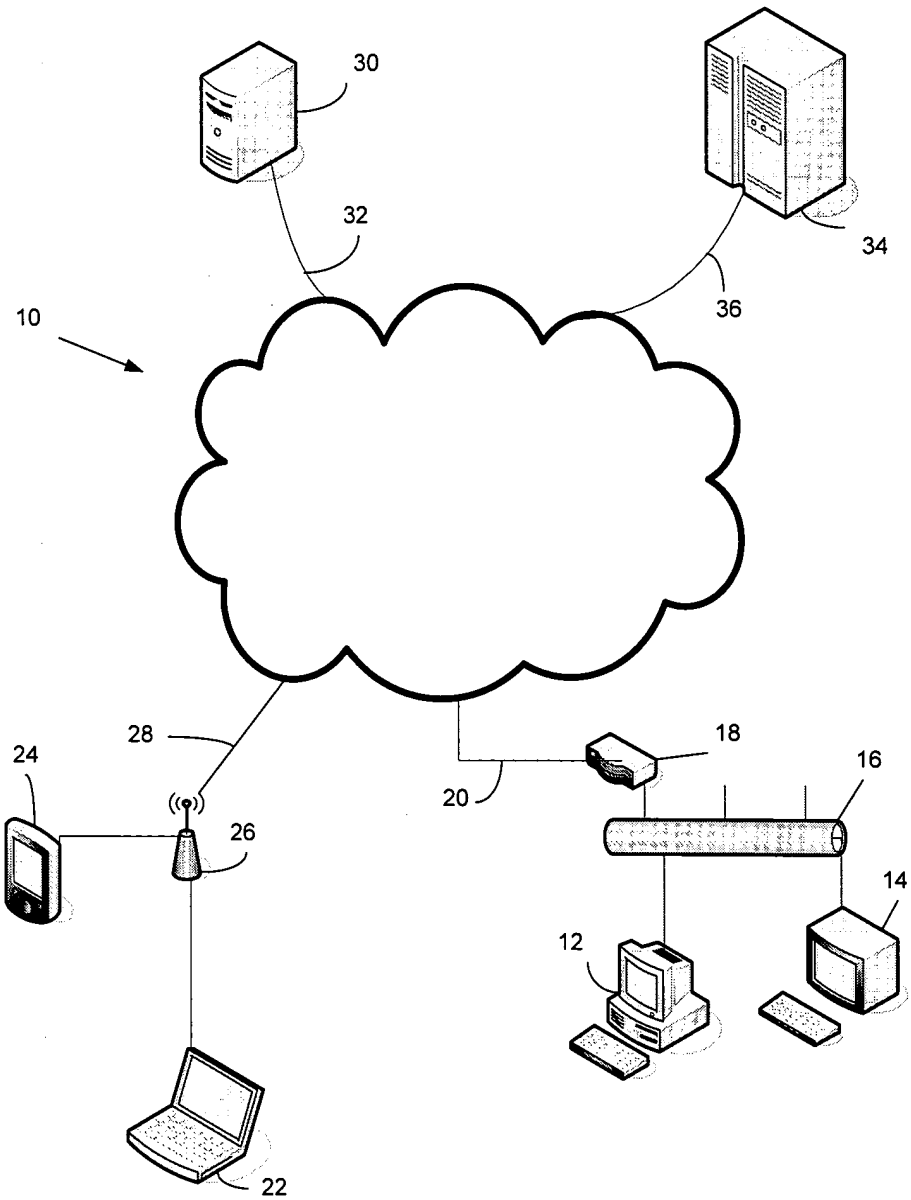


FIG. 1

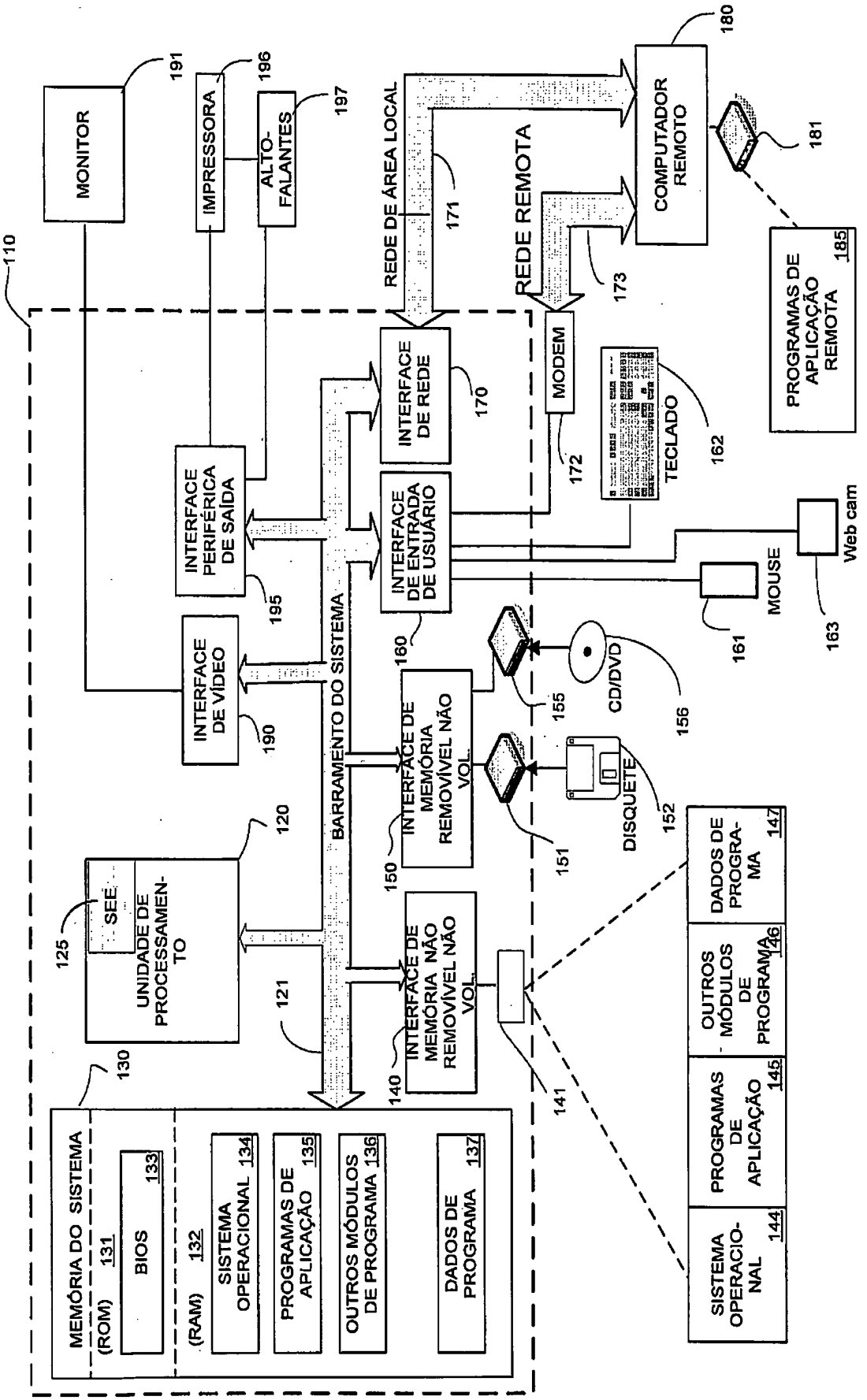

110
MONITOR
191
IMPRESSORA
196
ALTO-FALANTES
197
REDE DE ÁREA LOCAL
171
REDE REMOTA
COMPUTADOR REMOTO
180
181
PROGRAMAS DE APLICAÇÃO REMOTA
185
INTERFACE DE REDE
170
MODEM
172
173
TECLADO
162
INTERFACE PERIFÉRICA DE SAÍDA
195
INTERFACE DE ENTRADA DE USUÁRIO
160
MOUSE
161
Web cam
163
INTERFACE DE VÍDEO
190
BARRAMENTO DO SISTEMA
CD/DVD
156
155
DISQUETE
152
151
INTERFACE DE MEMÓRIA REMOVÍVEL NÃO VOL.
150
INTERFACE DE MEMÓRIA NÃO REMOVÍVEL NÃO VOL.
140
141
UNIDADE DE PROCESSAMENTO
120
SEE
125
121
130
MEMÓRIA DO SISTEMA
(ROM) 131
BIOS 133
(RAM) 132
SISTEMA OPERACIONAL 134
PROGRAMAS DE APLICAÇÃO 135
OUTROS MÓDULOS DE PROGRAMA 136
DADOS DE PROGRAMA 137
SISTEMA OPERACIONAL 144
PROGRAMAS DE APLICAÇÃO 145
OUTROS MÓDULOS DE PROGRAMA 146
DADOS DE PROGRAMA 147

FIG. 2

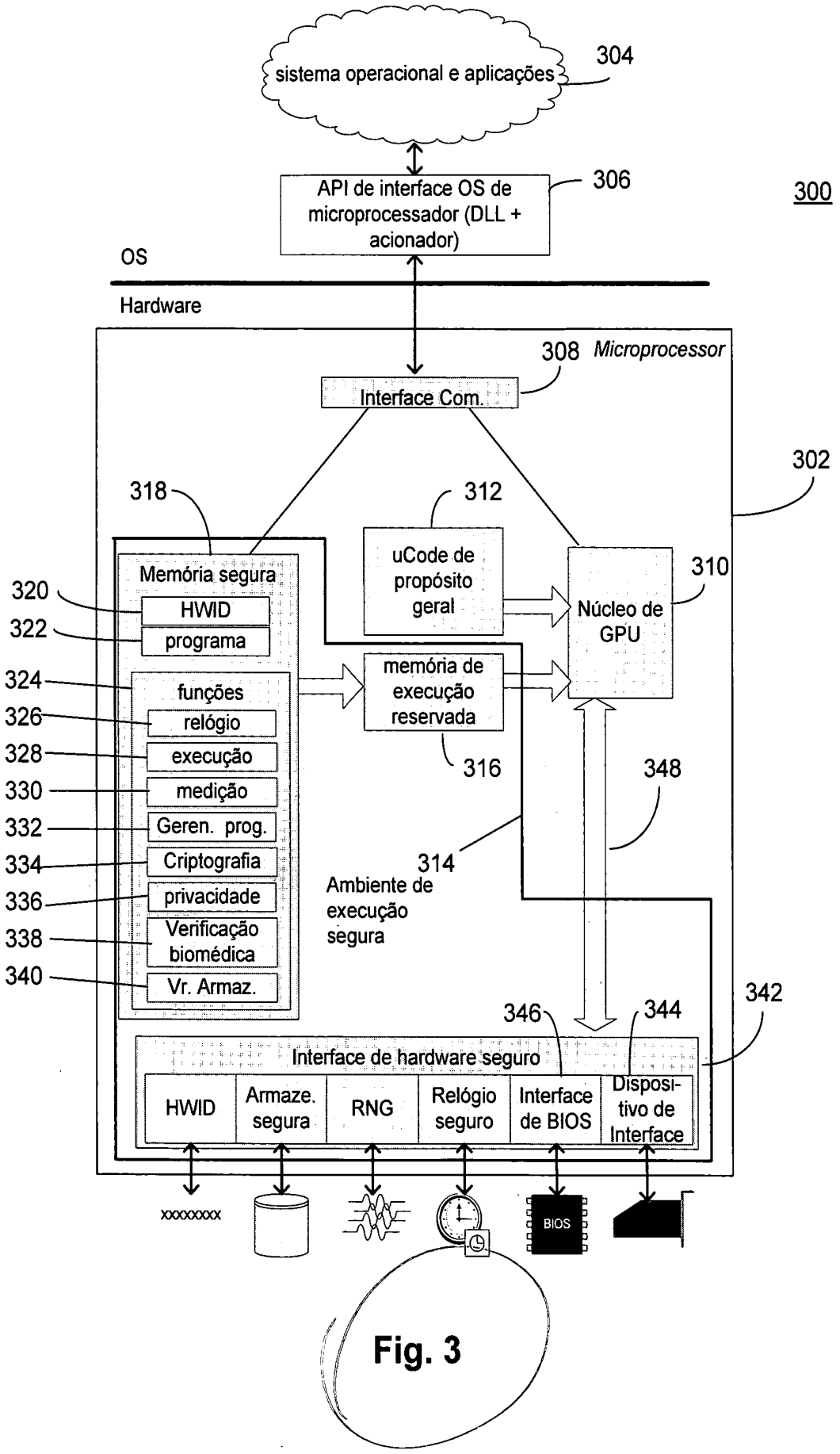

sistema operacional e aplicações
304
API de interface OS de microprocessador (DLL + acionador)
306
300
OS
Hardware
308 Microprocessor
Interface Com.
302
318
312
Memória segura
HWID
programa
funções
relógio
execução
medição
Geren. prog.
Criptografia
privacidade
Verificação biomédica
Vr. Armaz.
320
322
324
326
328
330
332
334
336
338
340
uCode de propósito geral
310
Núcleo de GPU
memória de execução reservada
316
348
314
Ambiente de execução segura
342
346
344
Interface de hardware seguro
HWID
Armaze. segura
RNG
Relógio seguro
Interface de BIOS
Dispositivo de Interface
xxxxxxxx
BIOS

Fig. 3

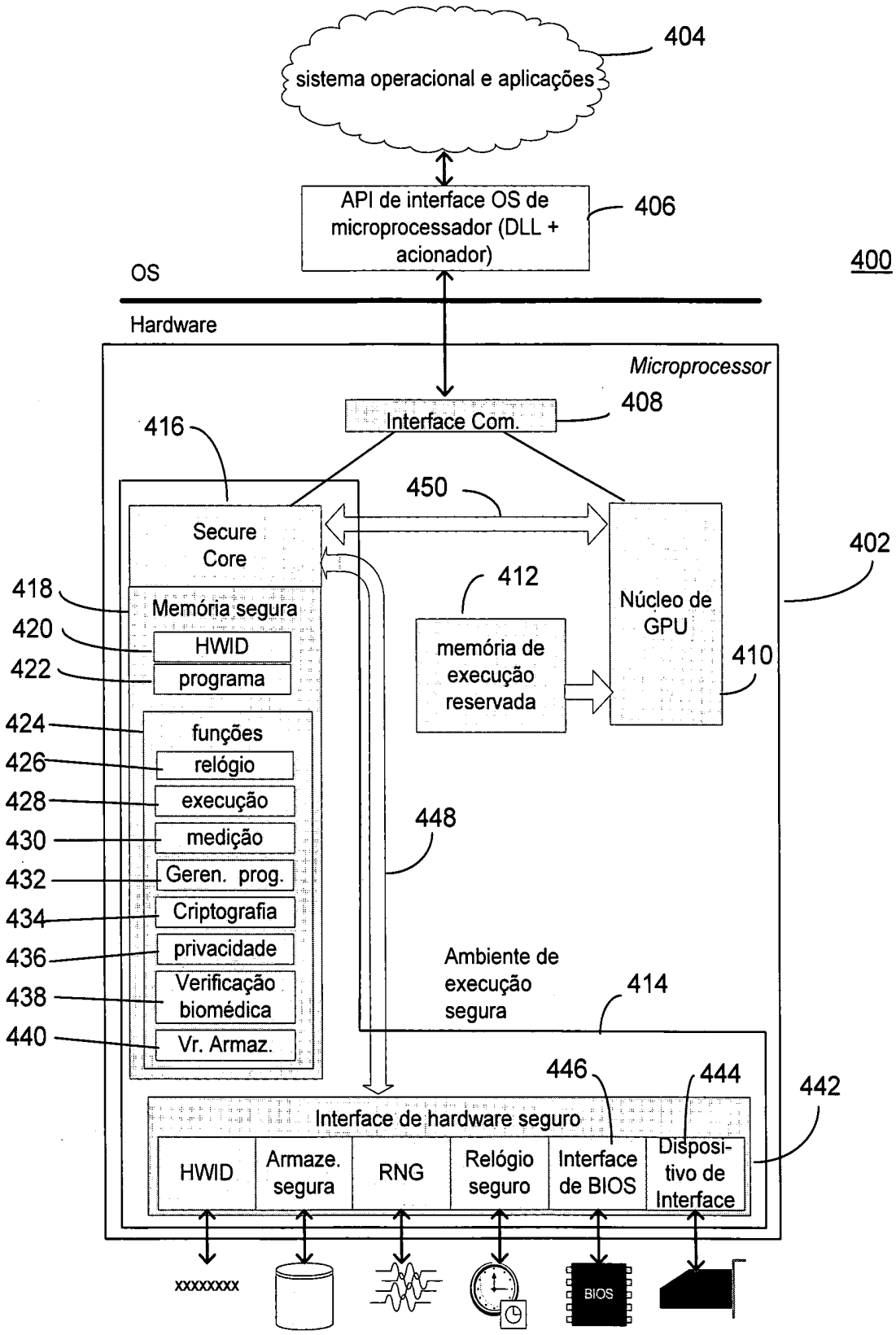

404
sistema operacional e aplicações
API de interface OS de microprocessador (DLL + acionador)
406
400
OS
Hardware
Microprocessor
Interface Com.
408
416
450
Secure Core
402
418
Memória segura
412
Núcleo de GPU
420
HWID
422
programa
memória de execução reservada
410
424
funções
426
relógio
428
execução
448
430
medição
432
Geren. prog.
434
Criptografia
436
privacidade
Ambiente de execução segura
414
438
Verificação biomédica
440
Vr. Armaz.
446
444
442
Interface de hardware seguro
HWID
Armaze. segura
RNG
Relógio seguro
Interface de BIOS
Disposi-tivo de Interface
xxxxxxxx
BIOS

Fig. 4

PI0615811-0

RESUMO

"SISTEMA OPERACIONAL ENCERRADO EM UNIDADE DE PROCESSAMENTO"

Uma unidade de processamento para uso em um dispositivo eletrônico inclui interfaces de comunicação e processamento de instrução padrão e também inclui capacidade funcional além de ou no lugar naquelas encontradas em um sistema operacional. Uma memória segura dentro da unidade de processamento pode conter um identificador de hardware, dados de programa, e funções de subsistema como um relógio seguro, gerenciamento de programa, e execução de programa. Os dados em funções dentro da memória de garantia não são acessíveis as partir do exterior da unidade de processamento.