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

(21) **PI0707225-2 A2**

BRPI0707225A2

(22) Data de Depósito: 19/01/2007
(43) Data da Publicação: 26/04/2011
(RPI 2103)

(51) Int.Cl.:
G06F 13/10
G06F 21/02

(54) Título: **REFORÇO BASEADO EM E/S DE MODOS DE OPERAÇÃO DE COMPUTADOR DE MÚLTIPLOS NÍVES**

(30) Prioridade Unionista: 14/02/2006 US 11/353,677

(73) Titular(es): Microsoft Corporation

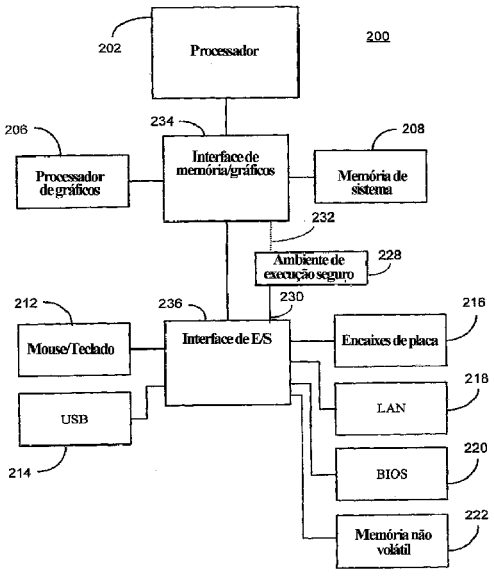
(72) Inventor(es): Alexander Frank, Isaac P. Ahdout, William J. Westerinen

(74) Procurador(es): Nellie Anne Daniel-shores

(86) Pedido Internacional: PCT US2007001504 de 19/01/2007

(87) Publicação Internacional: WO 2007/094918de 23/08/2007

(57) Resumo: REFORÇO BASEADO EM E/S DE MODOS DE OPERAÇÃO DE COMPUTADOR DE MÚLTIPLOS NÍVEIS. Um computador é arquitetado de maneira que uma monitoração e reforço de uma diretriz de operação são executadas em um circuito de interface que transmite dados entre um processador e um ou mais blocos de função. Os blocos de função podem incluir memória de sistema, um mostrador, uma rede, uma porta USB, ou uma memória não volátil. Uma vez que o circuito de interface manuseia cada transação entre o processador e seus blocos de função suportados, o circuito de interface é um ponto efetivo no qual para reforçar modos de desempenho limitado quando o uso do computador não está de acordo com a diretriz de operação.



PI0707225-2

"REFORÇO BASEADO EM E/S DE MODOS DE OPERAÇÃO DE COMPUTADOR DE MÚLTIPLOS NÍVEIS"

ANTECEDENTES

Modelos de negócios pré-pagos ou pós-pagos têm sido usados em muitas áreas de comércio, de telefones celulares a lavanderias automáticas comerciais. No desenvolvimento de um negócio pré-pago, um provedor, por exemplo, um provedor de telefone celular, oferece o uso de hardware (um telefone celular) em um custo inferior ao de mercado em troca de um compromisso de permanecer como um assinante de sua rede. Neste exemplo específico, o cliente recebe um telefone celular por pouco ou nenhum dinheiro em troca de assinar um contrato para se tornar um assinante por um dado período de tempo. Durante o curso do contrato o provedor de serviço recupera o custo do hardware ao carregar o consumidor para usar o telefone celular.

O modelo de negócio pré-pago é baseado no conceito de que o hardware fornecido tem pouco ou nenhum valor, ou uso, se desconectado do provedor de serviço. Para ilustrar, quando o assinante mencionado anteriormente pára de pagar a sua conta o provedor de serviço desativa sua conta e, embora o telefone celular possa ligar, chamadas não podem ser feitas por causa de o provedor de serviço não permitir. O telefone desativado não tem valor de "recuperação", porque o telefone não trabalhará em outro lugar e as partes de componente não são facilmente recuperadas nem elas têm um valor de mercado significativo. Quando a conta é colocada em dia, o provedor de serviço conectará de novo o dispositivo à rede

e permitirá execução de chamadas.

Este modelo funciona bem quando o provedor de serviço, ou outra entidade aceitando o risco financeiro de fornecer hardware subsidiado, tem um controle rígido do uso do hardware e quando o dispositivo tem pouco valor de recuperação. Este modelo de negócio não funciona bem quando o hardware tem substanciais usos fora da extensão de controle do provedor de serviço. Assim, um computador pessoal típico não satisfaz a estes critérios uma vez que um computador pessoal pode ter substanciais usos além de uma intenção original e os componentes de um computador pessoal, por exemplo, um mostrador ou unidade de disco, podem ter um valor de recuperação significativo.

Reforçar uma diretriz de operação que exija pagamento de taxas de assinatura ou taxas pós-pagas estimulará usuários a cumprir seus compromissos financeiros com um financiador que subsidia o preço de compra do computador. Entretanto, circuitos de reforço atrairão a atenção de hackers ou roubam os que desejam o benefício propriamente dito pelo furto de serviços de computador ou pelo furto do computador propriamente dito.

SUMÁRIO

Um computador configurado para automonitorar e reforçar obediência a uma diretriz de operação, tal como uma diretriz de operação pós-paga ou uma diretriz de operação de assinatura, pode usar um circuito de interface configurado para impedir acesso a circuitos periféricos e de suporte quando não obediência à diretriz de operação é determinada.

Quando o circuito de interface suporta memória de sistema ou a exibição, o reforço pode ser por meio de limitar a quantidade de memória disponível para execução de programa ou pode limitar a exibição com cores reduzidas ou um número reduzido de pixéis exibidos.

Quando o circuito de interface gerencia a maioria ou todas as outras entradas/saídas (E/S) de sistema, por exemplo, transferência de dados com portas de rede, interfaces seriais, encaixes de placa, memória não volátil, memória BIOS, um teclado e mouse e outros mais, o circuito de interface pode reforçar a diretriz de operação pela limitação de acesso entre qualquer um destes blocos de função e o processador. Limitar acesso neste caso pode incluir taxas de transferência de dados reduzidas, limites na transferência de dados, acesso de armazenamento somente de leitura ou somente de gravação, e acesso periférico restringido, para mencionar alguns. O resultado pode ser permitir uma faixa de sanções do mínimo ao máximo, dependendo da natureza da violação percebida, história de violação anterior, ou regras contratuais.

DESCRIÇÃO RESUMIDA DOS DESENHOS

A Figura 1 é um diagrama de blocos de um computador;

A Figura 2 é um diagrama de blocos de uma arquitetura de um computador similar ao computador da figura 1;

A Figura 2A é um diagrama de blocos de uma arquitetura alternativa do computador da figura 2; e

A Figura 3 é um circuito de interface adequado pa-

ra uso no computador das figuras 2 ou 2A.

DESCRIÇÃO DETALHADA

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 no final desta revelação. A descrição detalhada é para ser interpretada somente como exemplo e não descreve cada modalidade possível uma vez que descrever cada modalidade possível seria impraticável, se não impossível. Inúmeras modalidades alternativas podem ser implementadas, usando qualquer tecnologia atual ou tecnologia desenvolvida depois da data de depósito desta patente, que ainda estarão incluídas no escopo das reivindicações.

Também deve ser entendido que, a não ser que um termo esteja expressamente definido nesta patente usando a frase "Tal como usado neste documento, o termo '_' é por isto definido para significar..." ou uma frase similar, não existe intenção de limitar o significado desse termo, expressamente ou por implicação, além do seu significado comum ou usual, e tal termo não deve ser interpretado para ser limitado em escopo com base em qualquer declaração feita em qualquer seção desta patente (a não ser a linguagem das reivindicações). Para a extensão em que qualquer termo relatado nas reivindicações no final desta patente esteja referido nesta patente em um modo consistente com um único significado, o que é feito somente por motivo de clareza a fim de não confundir o leitor, não é pretendido que tal termo de reivindicação seja limitado, por implicação ou de outro modo,

àquele único significado.

Muito da inventiva funcionalidade e muitos dos princípios inventivos são melhores implementados com ou em softwares ou instruções e circuitos integrados (ICs) tais como ICs de aplicação específica. É esperado que um de habilidade usual, não obstante esforço possivelmente significativo e muitas opções de projeto motivadas, por exemplo, por tempo disponível, tecnologia atual e considerações econômicas, quando guiado pelos conceitos e princípios revelados neste documento será prontamente capaz de gerar tais instruções de software e programas e ICs com mínima experimentação. Portanto, no interesse de brevidade e minimização de qualquer risco de obscurecer os princípios e conceitos de acordo com a presente invenção, discussão adicional de tais softwares e ICs, se alguma, será limitada ao essencial com relação aos princípios e conceitos das modalidades preferidas.

Muitos computadores de alto valor, assistentes digitais pessoais, organizadores e outros mais de técnica anterior não são adequados para uso em um modelo de negócio pré-pago ou pós-pago assim como está. Tal como discutido anteriormente, tal equipamento pode ter valor significativo distante daqueles exigindo um provedor de serviço. Por exemplo, um computador pessoal pode ser desmontado e vendido como componentes, criando uma perda potencialmente significativa para o financiador de equipamento subsidiado. No caso onde um provedor de serviço da Internet financia o custo do computador pessoal com a expectativa de futuras taxas, este

"valor desprendido" cria uma oportunidade para subscrições fraudulentas e roubo. Modelos de negócio pré-pago, onde um usuário paga antecipadamente para uso de um ambiente de sistema de computação de alto valor subsidiado, têm riscos similares de fraude e roubo.

A Figura 1 ilustra um dispositivo de computação na forma de um computador 110 que pode ser conectado a uma rede, tal como a rede de área local 171 ou a rede de área estendida 173, e usado para hospedar um ou mais exemplos de um ambiente de execução seguro. Componentes do computador 110 podem incluir, mas não se limitando a estes, 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 à unidade de processamento 120. O barramento de sistema 121 pode ser qualquer um dos diversos tipos de estruturas de barramento incluindo um barramento de memória ou controlador de memória, um barramento periférico, e um barramento local usando qualquer uma de uma variedade de arquiteturas de barramento. A título de exemplo, e não de limitação, tais arquiteturas incluem barramento de Arquitetura Padrão da Indústria (ISA), barramento de Arquitetura de Micro Canal (MCA), barramento ISA Aprimorado (EISA), barramento local de Associação de Padrões Eletrônicos de Vídeo (VESA) e barramento de Interconexão de Componentes Periféricos (PCI) também conhecido como barramento Mezanino.

O computador 110 pode incluir um ambiente de execução seguro (SEE) 125. O SEE 125 pode ser capacitado para

executar monitoração de segurança, gerenciamento de uso pós-pago e assinatura e reforço de diretriz para termos e condições associados com uso pago, particularmente em um modelo de negócio de compra subsidiada. O ambiente de execução seguro 125 pode ser incorporado na unidade de processamento 120 ou como um componente autônomo tal como representado na figura 1. As funções detalhadas que podem ser suportadas pelo SEE 125 e modalidades adicionais do SEE 125 serão discutidas a seguir com relação à figura 3.

O computador 110 inclui tipicamente uma variedade de mídias legíveis por computador. Mídias legíveis por computador podem ser quaisquer mídias disponíveis que possam ser acessadas pelo computador 110 e incluem tanto mídias voláteis quanto não voláteis, mídias removíveis quanto não removíveis. A título de exemplo, e não de limitação, mídias legíveis por computador podem compreender mídias de armazenamento de computador e mídias de comunicação. Mídias de armazenamento de computador incluem mídias voláteis e não voláteis, removíveis e não removíveis implementadas em qualquer método ou tecnologia para armazenamento de informação tal como instruções legíveis por computador, estruturas de dados, módulos de programa ou outros dados. Mídias de armazenamento de computador incluem, mas não se limitando a estas, RAM, ROM, EEPROM, memória flash ou outra tecnologia de memória, CD-ROM, discos versáteis digitais (DVD) ou outro armazenamento de disco ótico, cassetes magnéticos, fita magnética, armazenamento de disco magnético ou outros dispositivos de armazenamento magnético, ou qualquer outra mídia

que possa ser usada para armazenar a informação desejada e que possa ser acessada pelo computador 110. Mídias de comunicação tipicamente incorporam instruções legíveis por computador, estruturas de dados, módulos de programa ou outros dados em um sinal de dados modulado tal como uma onda portadora ou outro mecanismo de transporte e incluem quaisquer mídias de entrega de informação. A expressão "sinal de dados modulado" significa um sinal que tenha uma ou mais das suas características estabelecidas ou mudadas de uma tal maneira como para codificar informação no sinal. A título de exemplo, e não de limitação, mídias de comunicação incluem mídias a fio tais como uma rede com fio ou conexão direta com fio, e mídias sem fio tais como acústica, radiofreqüência, infravermelho e outras mídias sem fio. Combinações de quaisquer das mencionadas anteriormente também devem ser incluídas no escopo de mídias legíveis por computador.

A memória de sistema 130 inclui mídias de armazenamento de computador na forma de memória volátil e/ou não volátil tais como a memória somente de leitura (ROM) 131 e a memória de acesso aleatório (RAM) 132. O sistema de entrada/saída básico (BIOS) 133, contendo as rotinas básicas que ajudam a transferir informação entre elementos dentro do computador 110, tal como durante a partida, é tipicamente armazenado na ROM 131. A RAM 132 tipicamente contém dados e/ou módulos de programa que são imediatamente acessíveis para a unidade de processamento 120 e/ou atualmente sendo operados por ela. A título de exemplo, e não de limitação, a figura 1 ilustra o sistema de operação 134, os programas de

aplicação 135, os outros módulos de programa 136 e os dados de programa 137.

O computador 110 também pode incluir outras mídias de armazenamento de computador removíveis/não removíveis, voláteis/não voláteis. Somente a título de exemplo, a figura 1 ilustra uma unidade de disco rígido 140 que lê mídias magnéticas não removíveis não voláteis ou grava nelas, uma unidade de disco magnético 151 que lê um disco magnético não volátil removível 152 ou grava nele, e uma unidade de disco ótico 155 que lê um disco ótico não volátil removível 156, ou grava nele, tal como um CD ROM ou outras mídias óticas. Outras mídias de armazenamento de computador removíveis/não removíveis, voláteis/não voláteis que podem ser usadas no ambiente de operação exemplar incluem, mas não se limitando a estas, cassetes de fita magnética, cartões de memória flash, discos versáteis digitais, fita de vídeo digital, RAM de estado sólido, ROM de estado sólido, e outras mais. A unidade de disco rígido 141 é tipicamente conectada ao barramento de sistema 121 por meio de uma interface de memória não removível tal como a interface 140, e a unidade de disco magnético 151 e a unidade de disco ótico 155 são tipicamente conectadas ao barramento de sistema 121 por uma interface de memória removível, tal como a interface 150.

As unidades e as suas mídias de armazenamento de computador associadas, discutidas anteriormente e ilustradas na figura 1, fornecem armazenamento de instruções legíveis por computador, estruturas de dados, módulos de programa e outros dados para o computador 110. Na figura 1, por exem-

plo, a unidade de disco rígido 141 está ilustrada como o sistema de operação de armazenamento 144, os programas de aplicação 145, os outros módulos de programa 146 e os dados de programa 147. Deve-se notar que estes componentes podem ser os mesmos ou diferentes de o sistema de operação 134, os programas de aplicação 135, os outros módulos de programa 136 e os dados de programa 137. Ao sistema de operação 144, programas de aplicação 145, outros módulos de programa 146 e aos dados de programa 147 são dados números diferentes aqui para ilustrar que, no mínimo, eles são cópias diferentes. Um usuário pode entrar com comandos e informação no computador 20 por meio de dispositivos de entrada tais como um teclado 162 e o dispositivo apontador 161, comumente referido como um mouse, mouse estacionário ou superfície sensível ao toque. Outros dispositivos de entrada (não mostrados) podem incluir um microfone, comando de jogos, controle manual de jogos, antena parabólica, digitalizador, ou coisa parecida. Estes e outros dispositivos de entrada são freqüentemente conectados à unidade de processamento 120 por meio de uma interface de entrada de usuário 160 que é acoplada ao barramento de sistema, mas podem ser conectados por outra interface e estruturas de barramento, tais como uma porta paralela, porta de jogos ou um barramento serial universal (USB). Um monitor 191 ou outro tipo de dispositivo de exibição também é conectado ao barramento de sistema 121 por meio de uma interface, tal como uma interface de vídeo 190. Além do monitor, computadores também podem incluir outros dispositivos periféricos de saída tais como os alto-falantes 197 e a im-

pressora 196, os quais podem ser conectados por meio de uma interface periférica de saída 190.

O computador 110 pode operar em um ambiente de rede usando conexões lógicas para um ou mais computadores remotos, tal como um computador remoto 180. O computador remoto 180 pode ser um computador pessoal, um servidor, um roteador, um PC de rede, um dispositivo de pares ou outro nó de rede comum, e inclui tipicamente muitos ou todos os elementos descritos anteriormente em relação ao computador 110, embora somente um dispositivo de armazenamento de memória 181 tenha sido ilustrado na figura 1. As conexões lógicas representadas na figura 1 incluem uma rede de área local (LAN) 171 e uma rede de área estendida (WAN) 173, mas também podem incluir outras redes. Tais ambientes de comunicação inter-rede são comuns em escritórios, redes de computadores estendidas de empresa, intranets e na Internet.

Quando usado em um ambiente de comunicação inter-rede LAN, o computador 110 é conectado à LAN 171 por meio de uma interface ou adaptador de rede 170. Quando usado em um ambiente de comunicação inter-rede WAN, o computador 110 inclui tipicamente um modem 172 ou outro dispositivo para estabelecer comunicações através da WAN 173, tal como a Internet. O modem 172, o qual pode ser interno ou externo, pode ser conectado ao barramento de sistema 121 por meio da interface de entrada de usuário 160, ou por outro mecanismo apropriado. Em um ambiente de rede, módulos de programa representados em relação ao computador 110, ou partes do mesmo, podem ser armazenados no dispositivo remoto de armazena-

mento de memória. A título de exemplo, e não de limitação, a figura 1 ilustra os programas de aplicação remota 185 como residindo no dispositivo de memória 181. Deve ser percebido que as conexões de rede mostradas são exemplares e que outros meios de se estabelecer um elo de comunicações entre os computadores podem ser usados.

A Figura 2 é um diagrama de blocos arquitetônico de um computador 200, o mesmo ou similar ao computador da figura 1. A arquitetura do computador 200 da figura 2 pode ser típica de computadores de uso geral amplamente vendidos e em uso atualmente. Um processador 202 pode ser acoplado a uma interface de gráficos e memória 204. A interface de gráficos e memória 204 pode ser um controlador "ponte norte" ou seu substituto funcional em arquiteturas mais recentes, tal como um "Circuito Controlador de Memória e Vídeo" (GMCH). A interface de gráficos e memória 204 pode ser acoplada ao processador 202 por meio de um barramento de dados de alta velocidade, tal como o "Barramento Frontal" (FSB), conhecido em arquiteturas de computador. O processador 202 também pode ser conectado, diretamente ou por meio da interface de gráficos e memória 204, a uma interface de entrada/saída 210 (interface E/S). A interface E/S 210 pode ser acoplada a uma variedade de dispositivos representados pelos componentes discutidos a seguir, mas não se limitando a estes. A interface E/S 210 pode ser uma microplaqueta "ponte sul" ou um circuito similar funcionalmente, tal como um "Circuito Controlador de E/S" (ICH). Diversos vendedores produzem circuitos ponte norte e ponte sul de técnica atual e suas equiva-

lências funcionais, incluindo a Intel Corporation.

Uma variedade de circuitos funcionais pode ser acoplada à interface de gráficos e memória 204 ou à interface E/S 210. A interface de gráficos e memória 204 pode ser acoplada à memória de sistema 206 e a um processador de gráficos 208, o qual pode ser conectado a um mostrador (não representado). Um mouse/teclado 212 pode ser acoplado à interface E/S 210. Um barramento serial universal (USB) 214 pode ser usado para fazer interface com periféricos externos incluindo memória flash, câmeras, adaptadores de rede, etc. (não representados). Os encaixes de placa 216 podem acomodar qualquer número de dispositivos de conexão, conhecidos e comuns na indústria. Uma interface de rede de área local (LAN) 218, tal como uma placa Ethernet pode ser conectada à interface E/S 210. Firmware, tal como um sistema de entrada/saída básico (BIOS) 220 pode ser acessado por meio da interface E/S 210. A memória não volátil 222, tal como uma unidade de disco rígido ou qualquer das outras memórias não voláteis listadas anteriormente, também pode ser acoplada à interface E/S 210.

Um ambiente de execução seguro 224 está mostrado disposto na interface E/S 210. Uma modalidade alternativa, mostrando um outro ambiente de execução seguro 226 disposto na interface de gráficos e memória 204, também está mostrada. Embora configurações de sistema com mais de um ambiente de execução seguro sejam suportados, uma modalidade é dirigida para um único exemplo do ambiente de execução seguro. Um circuito de interface com um ambiente de execução seguro

integral, tal como o ambiente de execução seguro 224 ou o ambiente de execução seguro 226 será discutido com mais detalhes com relação à figura 3.

A Figura 2A é uma modalidade alternativa do computador da figura 2. Nesta modalidade, um ambiente de execução seguro 228 não é disposto em um dos circuitos de interface 234 e 236, mas é uma unidade separada. O ambiente de execução seguro 228 pode ser acoplado à interface E/S 236 pelo barramento 230. De forma similar, quando configurado com a interface de gráficos e memória 234, o ambiente de execução seguro 228 pode ser acoplado à interface de gráficos e memória 234 por meio do barramento 232. Os barramentos separados 230 e 232 podem ser usados a fim de não interferir com as taxas de dados muito altas entre o processador 202, o controlador de gráficos e memória 234 e a interface E/S 236. Um barramento de menor velocidade pode satisfazer às exigências de uma implementação como esta, por exemplo, um barramento de circuito inter-integrado (IIC ou I^2C), conhecido na técnica. Quando configurados desta maneira, os barramentos 230 e 232 podem ter transferências de dados claras e dependem de dispositivos físicos para proteger os dados, tais como os barramentos sendo enterrados na placa de circuitos. Em uma outra modalidade, os dados nos barramentos 230 e 232 podem ser criptografados, exigindo suporte para comunicações seguras nos dois circuitos de interface 234, 236, respectivamente. Embora tal suporte possa ser inerente no ambiente de execução seguro 228, ele pode ser uma exigência adicional na interface de gráficos e memória 234 ou na interface E/S 236.

A Figura 3 é um diagrama de blocos de um circuito de interface exemplar 300, tal como o controlador de gráficos e memória 204 ou a interface E/S 210. O circuito de interface 300 pode incluir o conjunto real de circuitos de interface 302 tais como comutadores, multiplexadores e armazenamentos temporários que não estão representados. O circuito de interface 300 pode ser conectado diretamente ao um processador, tal como o controlador de gráficos e memória 204, ou pode ser conectado indiretamente por meio de um outro circuito, tal como a interface E/S 210, tal como mostrado na figura 2, ou pelos circuitos de interface 234 e 236 da figura 2A. Uma interface de barramento 306 pode fazer interface diretamente ou de forma indireta com o processador e as interfaces de barramento 308 e 310 podem se acoplar a uma variedade de circuitos funcionais, incluindo, mas não se limitando a estes, um processador de gráficos, memória de sistema, memória não volátil, E/S humana tal como o teclado e mouse, uma porta USB e conexões de comunicação inter-rede.

O circuito de interface 300 também pode incluir um ambiente de execução seguro 304 acoplado aos circuitos de interface. O ambiente de execução seguro 304 pode incluir uma memória segura 312 que pode ser usada para armazenar dados tais como um identificador de hardware 314, as configurações de diretrizes 316, o valor armazenado 318 e um registrador de estado 319. O identificador de hardware 314 pode identificar exclusivamente o ambiente de execução seguro particular e, por associação, o computador. A diretriz 316 pode incluir termos de uso e etapas progressivas de reforço

se os termos de uso forem violados. O valor armazenado 318 pode representar minutos de uso disponíveis, a data de término de uma assinatura mensal, ou pode representar valor real tal como créditos de compra que podem ser usados para uso ou compras não relacionadas, tais como acessórios.

O registrador de estado 319 pode armazenar um valor indicando o modo de operação do computador. Cada valor de estado pode representar um estado de operação diferente. Um valor de estado pode representar uso irrestrito, um outro valor de estado pode representar um modo de função reduzida que permite entrada de um pagamento, enquanto que um terceiro valor de estado pode representar um modo permitindo configuração de uma conexão de rede (configuração de rede pode ser exigida para permitir entrada de pagamento, e pode ser associada com o modo de entrada de pagamento). Um outro valor de estado pode representar um modo de função reduzida que permita recuperação de dados, permitindo recuperação de um sistema que tenha sido colocado em um modo restringido de operação. Um outro valor de estado pode representar um modo de operação mais restritivo que somente permite entrada de um código de recuperação, ou seja, uma mensagem assinada que pode ser interpretada diretamente pelo ambiente de execução seguro 304, e quando correta restaura o sistema para operação irrestrita. Também um outro valor de estado pode representar um modo incapacitado que não permite interação de usuário, mas em vez disto exige um técnico de serviço autorizado com acesso a ferramentas de hardware ou software especiais para reativar o computador. Estes últimos modos podem

restringir operação a um pequeno núcleo que tenha uma localização conhecida, tal como na memória segura 312 do ambiente de execução seguro 304. Referindo-se à figura 2, porque todo acesso de memória é por meio de um dos circuitos de interface 204 210, acesso do processador 202 a este núcleo especial pode ser reforçado pelo ambiente de execução seguro associado 226, 224 do circuito de interface 204, 210. Os modos de operação restringidos listados anteriormente podem compreender um conjunto de modos de operação restringidos que podem ser selecionado de acordo com a natureza do evento que dispara uma sanção e as exigências da diretriz atual com relação àquele evento.

O ambiente de execução seguro 304 também pode incluir um conjunto de funções 320 suportando operação pós-paga ou de assinatura. As funções podem ser implementadas em diversos modos, por exemplo, uma modalidade pode usar firmware tal como uma matriz de lógica programável e uma outra modalidade pode incluir um processador ou controlador (não representados) no ambiente de execução seguro para implementar as funções em software.

As funções 312 podem incluir, mas não se limitando a estas, um relógio 322 ou controlador de tempo implementando funções de relógio, as funções de reforço 324, a medição 326, o gerenciamento de diretriz 328, a criptografia 330, o gerenciamento de privacidade 332, a verificação biométrica 334, o valor armazenado 336 e a monitoração de obediência 338.

O relógio 322 pode fornecer uma base segura para

medição de tempo e pode ser usado como uma verificação contra um relógio de sistema mantido por um sistema de operação, tal como o sistema de operação 134 do computador 110 para ajudar impedir tentativas de fraude pela alteração do relógio de sistema. O relógio 322 também pode ser usado em conjunto com o gerenciamento de diretriz 328, por exemplo, para exigir comunicação com um servidor hospedeiro para verificar disponibilidade de atualização. As funções de reforço 324 podem ser executadas quando é determinado que o computador 110 não está de acordo com um ou mais elementos da diretriz 316. Tais ações podem incluir restringir acesso de memória de sistema pela realocação de uma maneira geral de memória de sistema disponível para um recurso não acessível, tal como o ambiente de execução seguro 224, 226. A memória de sistema 206 é tornada essencialmente indisponível para propósitos de usuário por este processo de realocação.

Uma outra função 320 pode ser a medição 326. A medição 326 pode incluir uma variedade de técnicas e medições, por exemplo, aquelas discutidas no co-pendente pedido de patente US 11/006.837. Quando ativar medição e quais itens específicos medir pode ser uma função da diretriz 316. A seleção de uma diretriz 316 apropriada e o gerenciamento de atualizações para a diretriz 316 podem ser implementados pela função de gerenciamento de diretriz 328. A função de gerenciamento de diretriz 328 pode solicitar e receber diretrizes atualizadas e ser responsável pela verificação de novas diretrizes, assim como pela sua instalação.

Uma função de criptografia 330 pode ser usada para

verificação de assinatura digital, assinatura digital, geração de número aleatório e encriptação/decriptação. Qualquer uma ou todas estas capacidades criptográficas podem ser usadas para verificar atualizações para a memória segura 312 ou para confiança estabelecida com uma entidade fora do ambiente de execução seguro 304, se dentro ou fora do computador 110.

O ambiente de execução seguro 304 pode permitir que diversas funções de propósito especial sejam desenvolvidas e usadas. Um administrador de privacidade 332 pode ser usado para gerenciar informação pessoal para um usuário ou grupo interessado. Por exemplo, o administrador de privacidade 332 pode ser usado para implementar uma função de "carteira" para reter endereço e dados de cartão de crédito para uso em compra de linha direta. Uma função de verificação biométrica 334 pode ser usada com um sensor biométrico externo (não representado) para verificar identidade pessoal. Tal verificação de identidade pode ser usada, por exemplo, para atualizar informação pessoal no administrador de privacidade 332 ou durante aplicação de uma assinatura digital. A função de criptografia 330 pode ser usada para estabelecer confiança e um canal seguro para o sensor biométrico externo.

Uma função de valor armazenado 336, em conjunto com o valor armazenado 318, também pode ser implementada para uso no pagamento para tempo ou subscrições em um computador pré-pago ou enquanto fazendo compras externas, por exemplo, em transações de comércio de mercadoria de linha direta.

A monitoração de obediência 338 pode ser um único teste ou uma combinação de testes. O teste ou testes podem ser usados para garantir a integridade do computador com relação à medição e a integridade total do hardware e software de computador, especificamente a integridade do ambiente de execução seguro 304. A monitoração de obediência 304 pode envolver funções que verifiquem versões de software específicas, por exemplo, uma versão do sistema de operação 134. Uma outra verificação de obediência pode verificar, para um computador pós-pago, que o tempo consumido (medido) é consistente com o tempo comprado como uma verificação de que a medição não está sendo adulterada.

Em uma modalidade, o computador 200 pode inicializar usando um procedimento de partida BIOS normal. Em um ponto quando o sistema de operação 134 está sendo ativado, a função de gerenciamento de diretriz 328 pode ser ativada. A função de gerenciamento de diretriz 328 pode determinar que a diretriz 316 atual é válida e então carregar os dados de diretriz 216. A diretriz 316 pode ser usada em um processo de configuração para configurar o computador 200 para operação. O processo de configuração pode incluir alocação de memória, capacidade de processamento, disponibilidade e uso de periférico assim como exigências de medição. Quando medição é para ser reforçada, diretrizes em relação à medição, tais como quais medições efetuar, podem ser ativadas. Por exemplo, medição por meio de uso de CPU (pós-pago) versus uso durante um período de tempo (assinatura), pode exigir diferentes medições. Adicionalmente, quando uso é carregado por

período ou por atividade, um balanço de valor armazenado 318 pode ser mantido usando a função de valor armazenado 336. Quando o computador 200 tiver sido configurado de acordo com a diretriz 316, o processo de inicialização normal pode continuar pela ativação e inicialização do sistema de operação 134 e dos outros programas de aplicação 135. Em outras modalidades, a diretriz 316 pode ser aplicada em pontos diferentes no processo de inicialização ou ciclo de operação normal.

Se não obediência à diretriz for descoberta, a função de reforço 324 pode ser ativada. Por causa de o gerenciamento de diretriz e as funções de reforço 328, 324 serem mantidas dentro do ambiente de execução seguro 304, alguns ataques típicos ao sistema são difíceis ou impossíveis. Por exemplo, a diretriz 316 não pode ser "enganada" pela substituição de uma seção de memória de diretriz da memória externa. De forma similar, o gerenciamento de diretriz e as funções de reforço 328, 324 não podem ser "subalimentados" pelo bloqueio de ciclos de execução ou bloqueio de suas respectivas faixas de endereços.

Funções de reforço específicas podem ser exigidas quando o tempo disponível é esgotado pelo uso normal, ou quando o computador cai em um estado de não obediência por acidente ou intenção. A função de medição 326 ou a função de obediência 338 pode mudar o registrador de estado 319 ajustando a partir desse uso irrestrito representante normal para um ajuste associado com reforço. O que pode fazer com que a função de reforço 324 seja ativada. Quando o ambiente de

execução seguro 304 é disposto em um circuito de interface ou acoplado a ele, tal como a interface de gráficos e memória 204 ou a interface E/S 210, uma faixa rica de opções de reforço pode ficar disponível. Por causa de os circuitos de interface serem bem posicionados para interagir com a maioria, se não todas, das funções do computador e porque os circuitos de interface 204, 210 se encontram entre aquelas funções e o processador, os circuitos de interface 204, 210 podem ser capazes de sintonizar finamente uma faixa de sanções, tal como necessário.

A interface de gráficos e memória 204 pode permitir sanções com base no envolvimento de memória de sistema e a saída de mostrador. Quando a memória de sistema 206 é sancionada, a memória de sistema disponível para uso pelo processador 202 pode ser cortada dramaticamente, para menos que 25% da memória de sistema normalmente disponível. O impacto pode ser tornar lento o processamento ou limitar funções avançadas tais como edição de imagem. Uma outra sanção envolvendo a memória de sistema 206 pode ser limitar a memória a uma quantidade fixada, por exemplo, de 512 MB para 10 MB. Se troca de página também for restringida o programa que pode ser suportado pode ser sintonizado pela elevação e diminuição da quantidade de memória fixada, com a menor quantidade de memória correspondendo a uma limitação mais severa na função do computador 200.

Quando o mostrador é sancionado, a interface de gráficos e memória 204 pode limitar os dados enviados para o processador de gráficos 208 ou pode enviar ajustes de confi-

guração que neutralizem configurações de usuário existentes. Por exemplo, o número de pixéis pode ser limitado ou a profundidade de cor pode ser reduzida, dependendo das exigências da diretriz relacionada com aquele estado de operação. Uma outra sanção pode envolver intervalo de tempo para o mostrador depois de um intervalo a partir da inicialização, por exemplo, 10 minutos, permitindo execução de funções de recuperação, mas limitando períodos de trabalho útil.

A interface E/S 224 oferece mais oportunidades para impor uma sanção pela limitação da função do computador 200. A memória não volátil 222 pode ser limitada a somente de acesso de leitura, permitindo carregar programas, ou dados a ser copiados, mas não permitindo troca de página para disco ou dados de usuário a ser armazenados. Para esta sanção ser inteiramente efetiva as conexões LAN 218 e as portas USB 214 também podem ser restringidas. Quando uma sanção somente de leitura também pode ser severa, acesso de memória não volátil pode ser estabelecido para permitir acesso de leitura em velocidade total e acesso de gravação em uma taxa muito inferior, por exemplo, menos que 10% da taxa de leitura. O estabelecimento de direção de dados ou limitação de taxas de dados pode ser realizado pela desativação (por exemplo, estabelecimento para estado triplo) de armazenamentos temporários de dados de barramento de gravação. O estabelecimento de taxas de dados pode ser realizado pela mudança das taxas de relógio para armazenamentos temporários de dados na interface.

Um outro método para limitar a efetividade de uma

função pode ser avaliar o tipo de dados sendo acessado e permitir acesso a arquivos de dados, mas bloquear acesso a arquivos executáveis. E utilidade isenta, tal como uma rotina de recuperação, pode então fornecer acesso limitado aos arquivos de dados para propósitos de recuperação. Em uma outra modalidade, efetividade de memória não volátil pode ser limitada pela diminuição do acesso de leitura para uma taxa muito baixa para desencorajar qualquer uso a não ser para acrescentar valor ou de outro modo pegar etapas para restaurar operação normal. Uma taxa de dados lenta como esta pode ser menos que 1% da velocidade normalmente suportada, ou em uma modalidade, uma taxa fixada de 10 KB/s.

A interface E/S 210 também pode limitar a efetividade de uma de suas funções conectadas ao desabilitar comunicação com a rede de área local 218. Isto pode bloquear acesso à Internet ou a uma rede local. Alternativamente, em vez de desabilitar comunicação de rede de área local, velocidades de transferência de dados podem ser restringidas, ou um limite de volume total máximo de dados transferidos durante um período de tempo pode ser imposto.

Similar às outras restrições de transferência de dados, transferências de dados através da porta USB 214 podem ser bloqueadas ou restringidas. Por causa de a porta USB 214 poder ser usada para uma variedade de periféricos, o impacto pode se estender a um teclado ou mouse, um cartão de memória, uma câmera digital, uma rede sem fio, ou a outro dispositivo. Tal como indicado anteriormente, bloqueio ou limitação de taxas de transferência de dados pode ser reali-

zado ao bloquear ou abaixar a taxa de relógio em armazenamentos temporários de dados na interface E/S 210.

Para reverter o computador 200 para operação normal, um código de restauração pode necessitar ser adquirido de uma autoridade de licenciamento ou provedor de serviço (não representado) e fornecido como entrada para o computador 300. O código de restauração pode incluir o ID de hardware 320, uma renovação de valor armazenado, e uma data "não mais cedo do que" usada para verificar o relógio 322. O código de restauração tipicamente pode ser criptografado e assinado para confirmação pela unidade de processamento 302.

Um ambiente de execução seguro pode ser distinguido de uma base de computação confiável (TCB) ou de base de computação segura de próxima geração (NGSCB) em que o ambiente de execução seguro não tenta limitar adição de recursos ou funções ao computador, nem ele tenta proteger o computador contra vírus, programas mal intencionados, ou outros efeitos laterais indesejáveis que podem ocorrer em uso. O ambiente de execução seguro tenta proteger os interesses de um financiador ou proprietário de recurso para assegurar que termos de negócio, tais como pós-pago ou subscrições, sejam satisfeitos e para desencorajar roubo ou furto do computador como um todo ou em parte.

REIVINDICAÇÕES

1. Computador adaptado para operação em um modo de uso irrestrito e em um modo de função limitado, **CARACTERIZADO** pelo fato de que compreende:

um processador;

uma pluralidade de circuitos funcionais; e

um circuito de suporte acoplado ao processador e a pelo menos um da pluralidade de circuitos funcionais, o circuito de suporte compreendendo:

uma interface para gerenciar comunicação de dados entre o processador e o pelo menos um da pluralidade dos circuitos funcionais;

uma função de estado refletindo um status de obediência e para enviar um sinal ativando um modo limitado de operação de função; e

uma função de reforço para ajustar a interface para impedir desempenho efetivo do pelo menos um da pluralidade de circuitos funcionais responsivos ao sinal para ativar o modo limitado de operação de função.

2. Computador, de acordo com a reivindicação 1, **CARACTERIZADO** pelo fato de que o modo de função limitado é selecionado de um conjunto de modos de função limitados compreendendo um de:

a) entrar com um pagamento;

b) configurar uma conexão de rede;

c) recuperar dados;

d) desabilitar o computador, mas permitir entrada de usuário de um código de recuperação; e

e) desabilitar o computador e exigir intervenção de técnico de serviço autorizado.

3. Computador, de acordo com a reivindicação 2, **CARACTERIZADO** pelo fato de que a função de reforço capacita o modo de função limitado selecionado por controlar pelo menos um de acesso de entrada/saída e disponibilidade de memória.

4. Computador, de acordo com a reivindicação 2, **CARACTERIZADO** pelo fato de que a função de estado compreende uma função de medição e em que a função de reforço seleciona o modo de função limitado do conjunto de modos de função limitados responsivos a um sinal da função de medição indicando um nível de reforço.

5. Método para limitar o desempenho de um computador, **CARACTERIZADO** pelo fato de que compreende:

monitorar um evento de disparo correspondente a ativar um modo restringido de operação;

selecionar um modo restringido de operação do computador de um conjunto de modos restringidos de operação responsivos ao evento de disparo;

ativar o modo restringido de operação selecionado pela limitação de uma efetividade uma função em um circuito de interface que acopla a função a um processador.

6. Método, de acordo com a reivindicação 5, **CARACTERIZADO** pelo fato de que a função compreende pelo menos um de uma função de memória de sistema, uma função de exibição, uma função de acesso de memória não volátil, um Barramento Serial Universal e uma função de interface de rede.

7. Método, de acordo com a reivindicação 5, **CARACTERIZADO** pelo fato de que a função é uma função de memória de sistema e limitar a efetividade da função compreende limitar memória de sistema a menos que 25% de uma memória de sistema normalmente disponível.

8. Método, de acordo com a reivindicação 5, **CARACTERIZADO** pelo fato de que a função é uma função de memória de sistema e limitar a efetividade da função compreende limitar memória de sistema a uma quantidade fixada de memória disponível para processamento, em que uma limitação mais severa de funcionalidade é alcançada pela diminuição da quantidade fixada de memória disponível para processamento.

9. Método, de acordo com a reivindicação 5, **CARACTERIZADO** pelo fato de que a função é uma função de exibição e limitar a efetividade da função compreende pelo menos um de reduzir um número de pixéis disponíveis para exibir informação, reduzir a profundidade/espectro de cor disponível e automaticamente interromper o sinal de exibição no final de um intervalo.

10. Método, de acordo com a reivindicação 5, **CARACTERIZADO** pelo fato de que a função é uma função de acesso de memória não volátil e limitar a efetividade da função compreende pelo menos um de limitar o tamanho disponível de memória não volátil, limitar acesso de dados a dados somente de leitura, limitar acesso de dados para somente de gravação, limitar velocidade de acesso de dados e limitar tamanho acumulado de acesso de dados por inicialização/restauração.

11. Método, de acordo com a reivindicação 5, **CARACTERIZADO** pelo fato de que a função é uma função de acesso de memória não volátil e limitar a efetividade da função compreende limitar acesso de dados para ler em velocidade total e gravar em uma taxa menor que 10% da taxa de leitura.

12. Método, de acordo com a reivindicação 5, **CARACTERIZADO** pelo fato de que a função é uma função de acesso de memória não volátil e limitar a efetividade da função compreende fornecer acesso limitado a arquivos de dados e nenhum acesso a arquivos executáveis.

13. Método, de acordo com a reivindicação 5, **CARACTERIZADO** pelo fato de que a função é uma função de acesso de memória não volátil e limitar a efetividade da função compreende limitar acesso de dados a dados somente de leitura em uma taxa de dados restringida comparada a uma taxa de dados disponível durante operação normal.

14. Método, de acordo com a reivindicação 5, **CARACTERIZADO** pelo fato de que a função é uma função de interface de rede e limitar a efetividade da função compreende um de bloquear acesso a uma rede, limitar uma velocidade de transferência de dados e limitar um total de dados transferidos durante um período de tempo.

15. Método, de acordo com a reivindicação 5, **CARACTERIZADO** pelo fato de que a função é um Barramento Serial Universal e limitar a efetividade da função compreende limitar uma transferência de dados através do USB para somente gravação.

16. Circuito de suporte em um computador para processar sinais carregando dados entre um processador e pelo menos um bloco de função do computador, **CARACTERIZADO** pelo fato de que compreende:

uma pluralidade de barramentos bidirecionais para enviar e receber dados;

um circuito de interface para processar e rotear os sinais entre a pluralidade de barramentos;

um ambiente de execução para monitorar obediência a uma diretriz de operação e reforçar a diretriz de operação quando o computador não está de acordo com a diretriz de operação.

17. Circuito de suporte, de acordo com a reivindicação 16, **CARACTERIZADO** pelo fato de que o ambiente de execução compreende um circuito de reforço acoplado ao circuito de interface, em que o circuito de reforço faz com que o circuito de interface limite processamento e roteamento dos sinais entre a pluralidade de barramentos.

18. Circuito de suporte, de acordo com a reivindicação 16, **CARACTERIZADO** pelo fato de que o ambiente de execução compreende uma função criptográfica para uso no processamento de mensagens recebidas no ambiente de execução.

19. Circuito de suporte, de acordo com a reivindicação 16, **CARACTERIZADO** pelo fato de que o ambiente de execução ativa um modo de função limitado do computador selecionado de um conjunto de modos de função limitados, a seleção correspondendo a um grau de não obediência com a diretriz de operação.

20. Circuito de suporte, de acordo com a reivindicação 16, **CARACTERIZADO** pelo fato de que o ambiente de execução compreende uma porta para sinalizar uma função de reforço externa quando o computador não está de acordo com a diretriz de operação.

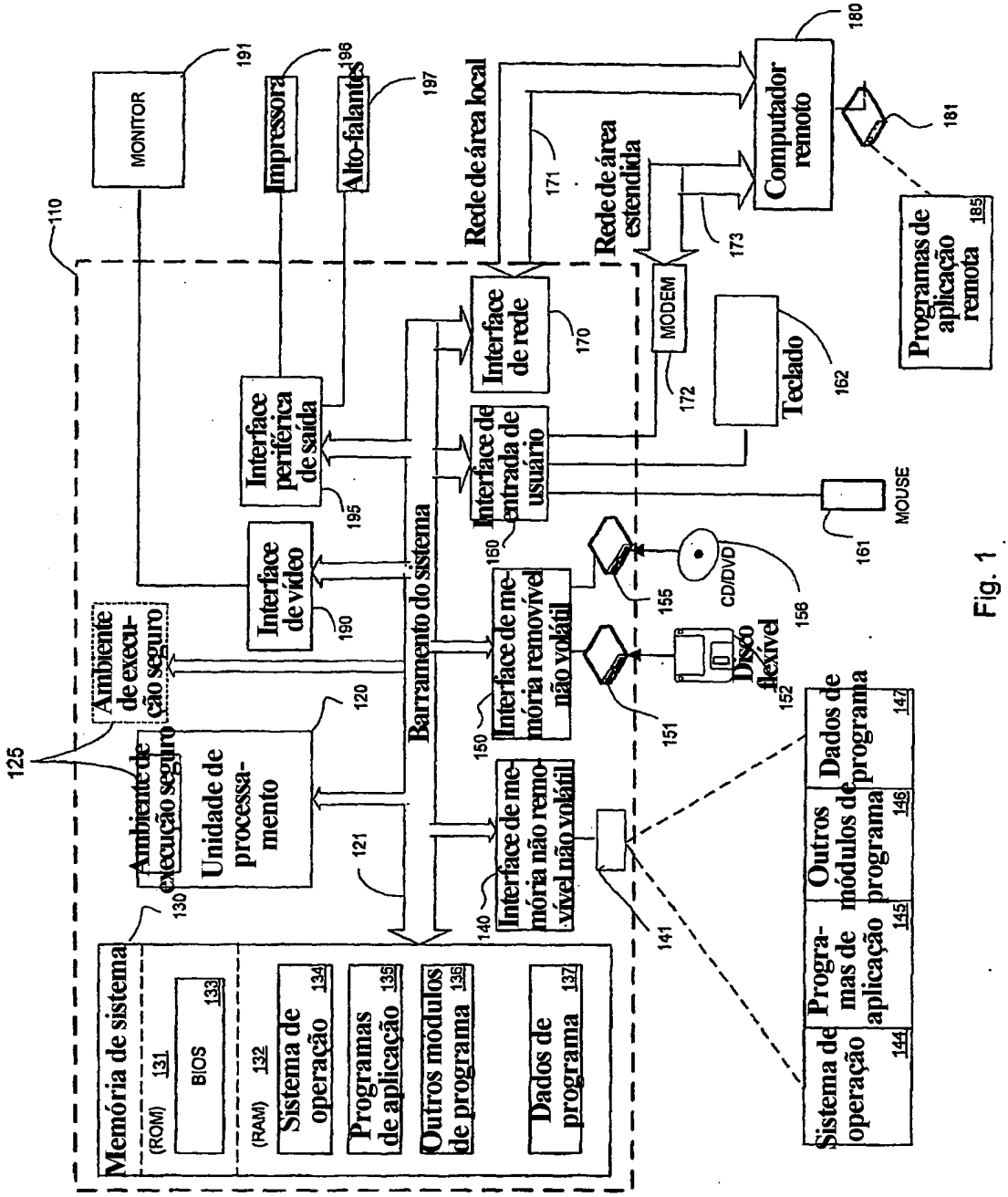

125
110
Ambiente de execução seguro
Ambiente de execução seguro
130
Memória de sistema
(ROM) 131
BIOS 133
(RAM) 132
Sistema de operação 134
Programas de aplicação 135
Outros módulos de programa 136
Dados de programa 137
Unidade de processamento
120
121
Barramento do sistema
Interface de vídeo
190
MONITOR
191
Interface periférica de saída
195
Impressora
196
Alto-falantes
197
Interface de memória não removível não volátil
140
141
Interface de memória removível não volátil
150
151
Interface de rede
170
Rede de área local
171
Interface de entrada de usuário
160
Rede de área estendida
MODEM
172
173
Computador remoto
180
181
Programas de aplicação remota
185
Teclado
162
MOUSE
161
CD/DVD
155
158
Disco flexível
152
Sistema de operação 144
Programas de aplicação 145
Outros módulos de programa 146
Dados de programa 147

Fig. 1

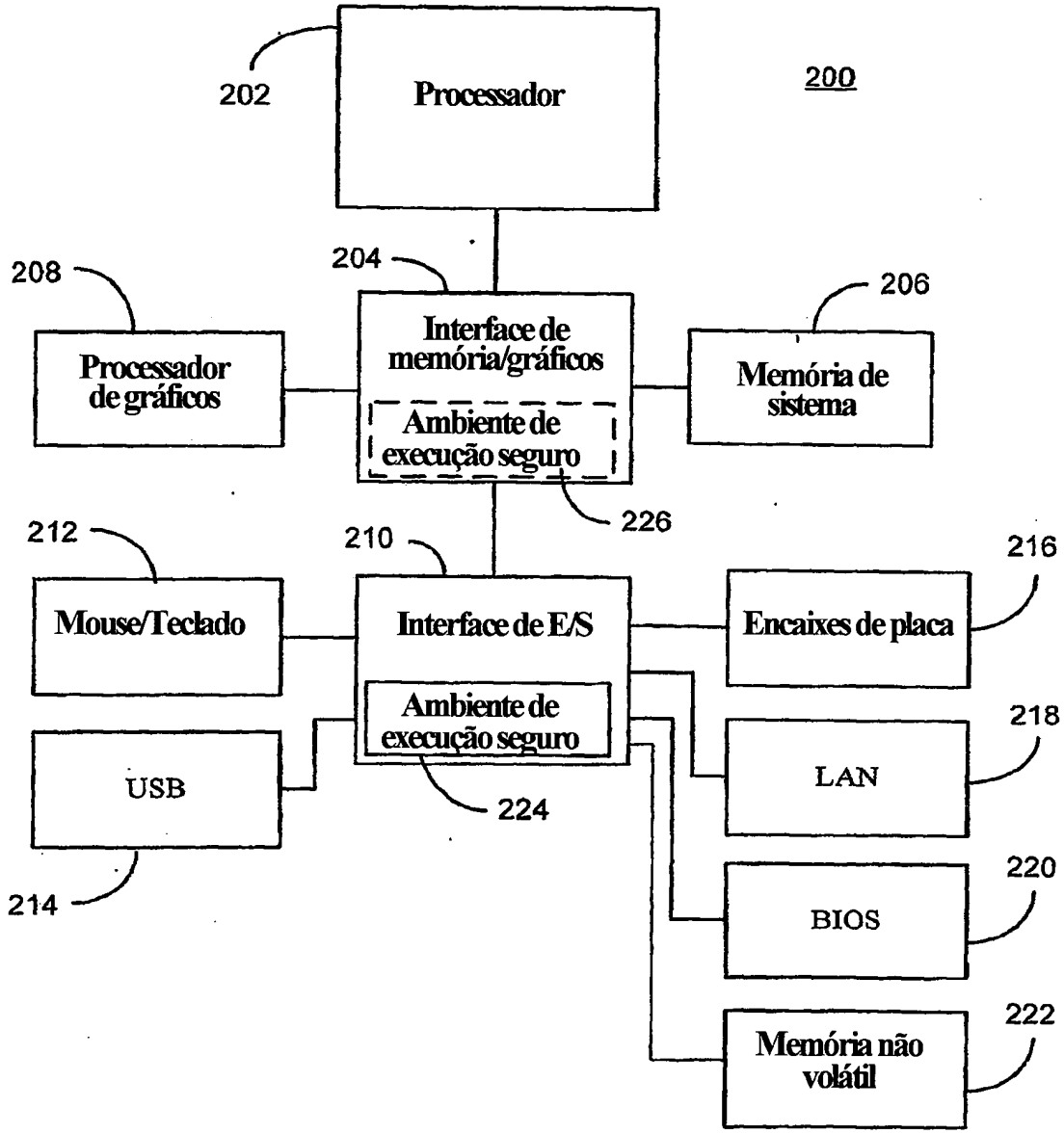

202
Processador
200
208
204
206
Processador de gráficos
Interface de memória/gráficos
Ambiente de execução seguro
Memória de sistema
226
212
210
216
Mouse/Teclado
Interface de E/S
Encaixes de placa
Ambiente de execução seguro
218
USB
LAN
224
220
BIOS
214
222
Memória não volátil

Fig. 2

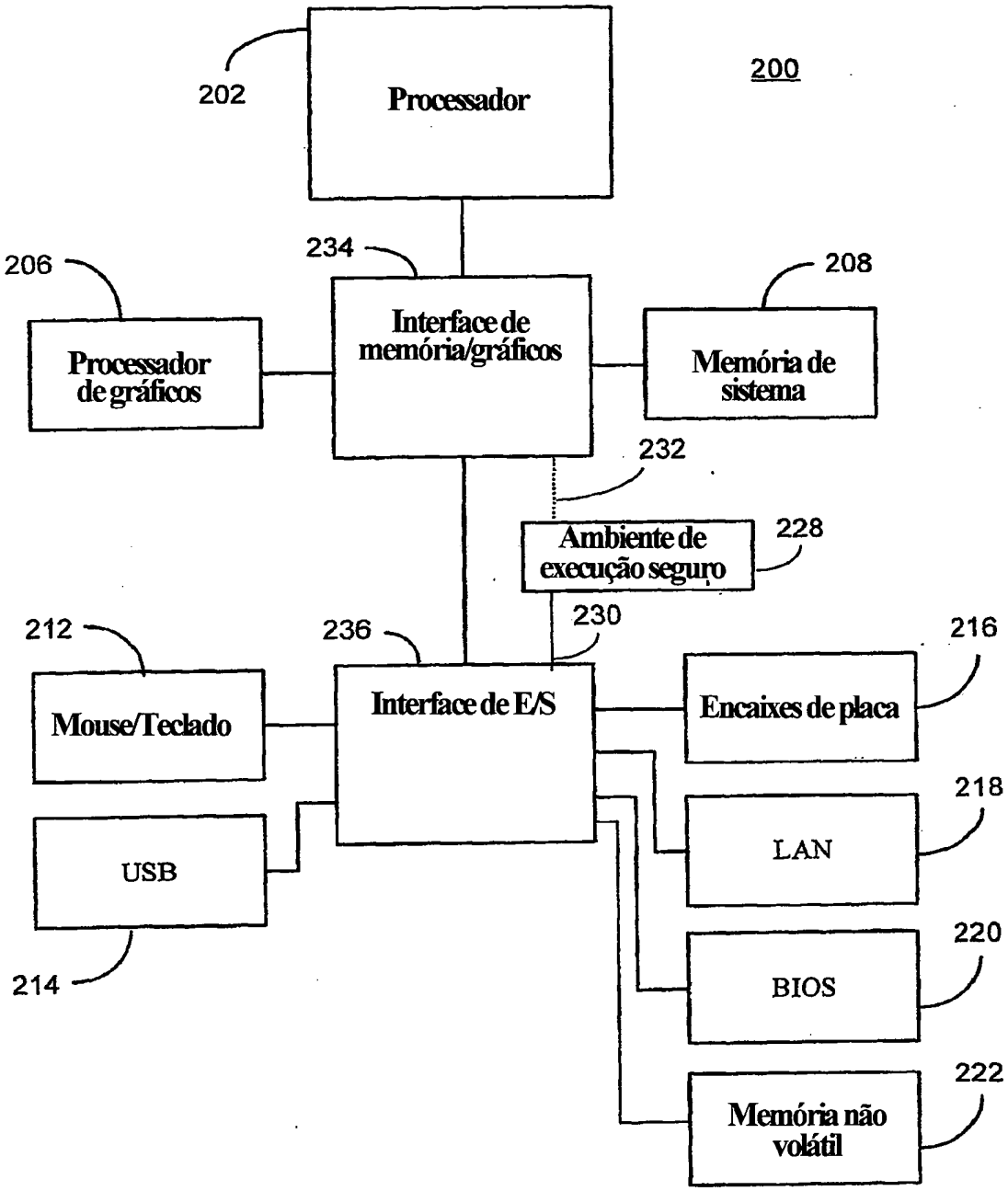

200
202
Processador
234
206
208
Interface de memória/gráficos
Processador de gráficos
Memória de sistema
232
Ambiente de execução seguro
228
212
236
230
216
Mouse/Teclado
Interface de E/S
Encaixes de placa
218
LAN
USB
220
BIOS
214
222
Memória não volátil

Fig. 2A

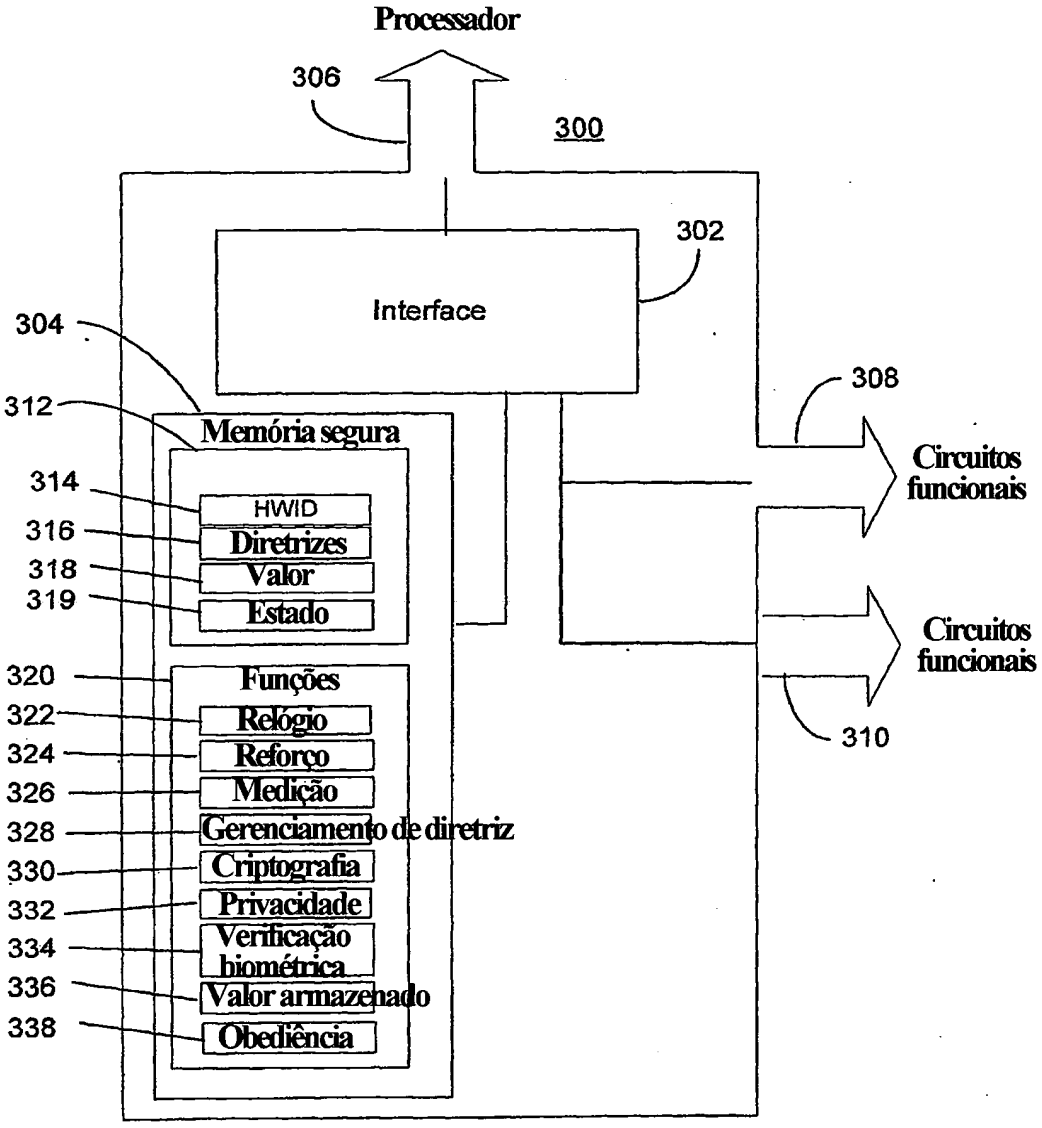

Processador
306
300
302
Interface
304
312
Memória segura
314
HWID
316
Diretrizes
318
Valor
319
Estado
320
Funções
322
Relógio
324
Reforço
326
Medição
328
Gerenciamento de diretriz
330
Criptografia
332
Privacidade
334
Verificação biométrica
336
Valor armazenado
338
Obediência
308
Circuitos funcionais
Circuitos funcionais
310

Fig. 3

RESUMO

"REFORÇO BASEADO EM E/S DE MODOS DE OPERAÇÃO DE COMPUTADOR DE MÚLTIPLOS NÍVEIS"

Um computador é arquitetado de maneira que uma monitoração e reforço de uma diretriz de operação são executadas em um circuito de interface que transmite dados entre um processador e um ou mais blocos de função. Os blocos de função podem incluir memória de sistema, um mostrador, uma rede, uma porta USB, ou uma memória não volátil. Uma vez que o circuito de interface manuseia cada transação entre o processador e seus blocos de função suportados, o circuito de interface é um ponto efetivo no qual para reforçar modos de desempenho limitado quando o uso do computador não está de acordo com a diretriz de operação.