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

# (21) PI 0720470-1 A2

* B R P I 0 7 2 0 4 7 0 A 2 *

(22) Data de Depósito: 18/12/2007
**(43) Data da Publicação: 14/01/2014**
**(RPI 2245)**

***(51) Int.Cl.:***
**G06F 1/26**
**G06F 11/18**

**(54) Título:** IMPOSIÇÃO DE SUBMISSÃO NO COMPUTADOR

**(57) Resumo:**

**(30) Prioridade Unionista:** 18/12/2006 US 11/612.435

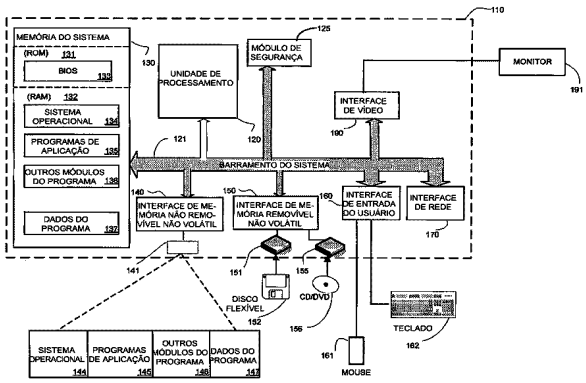
**(73) Titular(es):** Microsoft Corporation

**(72) Inventor(es):** Alexander Frank, Shon Schmidt, Stephen Richard Drake, Todd L. Carpenter, William J. Westerinen

**(74) Procurador(es):** Nellie Anne Daniel-Shores

**(86) Pedido Internacional:** PCT US2007087875 de 18/12/2007

**(87) Publicação Internacional:** WO 2008/077010de 26/06/2008



"IMPOSIÇÃO DE SUBMISSÃO NO COMPUTADOR"

ANTECEDENTES

Modelos de negócios de "pagamento quando você usa" ou "pagamento por usar" têm sido usados em muitas áreas de comércio, de telefones celulares a lavanderias comerciais. No desenvolvimento de um negócio de "pagamento quando você usa", um provedor, por exemplo, um provedor de telefone celular, oferece o uso do hardware (um telefone celular) em um custo menor do que o mercado na troca por um comprometimento de permanecer um assinante na sua rede por um período de tempo. Nesse exemplo específico, o consumidor recebe um telefone celular por pouco ou nenhum dinheiro em troca pela assinatura de um contrato para se tornar um assinante por um dado período de tempo. Através do decorrer do contrato, o provedor do serviço recupera o custo do hardware cobrando o consumidor pelo uso do telefone celular.

O modelo de negócio de "pagamento quando você usa" é baseado no conceito que o hardware provido tem pouco ou nenhum valor, ou uso, se desconectado do provedor de serviço. Para ilustrar, caso o assinante mencionado acima pare de pagamento a sua conta, o provedor de serviço desativa a conta, e embora o telefone celular possa ligar, chamadas não podem ser feitas porque o provedor de serviço não as permitirá. O telefone desativado não tem valor de "recuperação", porque o telefone não funcionará em outro lugar e as partes de componente não são facilmente recuperadas nem elas têm um valor simples significativo. Na maior parte dos casos, entretanto, mesmo embora o telefone tenha sido desativado, ele é ainda capaz de se conectar no provedor de serviço de modo a conciliar a restauração da conta. Quando a conta é ativada, o provedor do serviço autorizará novamente o dispositivo na sua rede e permitirá chamadas.

Esse modelo funciona bem quando o provedor de serviço, ou outra entidade aceitando o risco financeiro de prover hardware subsidiado, é capaz de impor os termos do contrato como acima, isto é, limitando o uso do dispositivo a somente essas funções requeridas para restaurar a conta. Quando o dispositivo é mais complexo, tal como um computador, meramente limitar o acesso a uma rede pode não ser suficiente para forçar um assinante a obedecer aos termos de um contrato.

SUMÁRIO

A forma mais simples, e possivelmente mais efetiva, de imposição quando um usuário de computador de pagamento por uso ou de assinatura falha em satisfazer as obrigações contratuais é apenas desativar ou paralisar o computador. Entretanto, uma tal medida pode ser difícil para se recuperar, caso os termos do contrato posteriormente sejam satisfeitos. Mais desejável é um mecanismo altamente resistente a falsificação para reduzir a função do computador até uma tal extensão que um processo de restauração seja a única operação prática a executar.

Um módulo de segurança pode ser usado para gerenciar imagens de BIOS, força e a atividade do barramento. O módulo de segurança pode ter mais do que um BIOS para uso dependendo de se as colocações feitas antes de uma inicialização corrente indicam operação normal, de uso medido ou restrita, adequada somente para reativar o computador. Se a operação restrita é indicada, um BIOS de operação restrita pode ser selecionado e carregado. O BIOS da operação restrita ajusta a memória do sistema para uma quantidade muito limitada, por exemplo, 4 megabytes. A memória do sistema pode ser ajustada para qualquer tamanho que permita a operação de uma pequena aplicação de restauração do sistema, mas seja muito pequena para permitir a execução de um sistema operacional, jogo ou outra aplicação do usuário benéfica. Para ajudar a garantir que o BIOS selecionado tenha tempo para executar as suas atividades de configuração do sistema com oportunidade minimizada para interferência, o módulo de segurança pode também gerenciar a força para os circuitos não essenciais do computador, tal como um circuito integrado de I/O. Quando um botão de força é pressionado, essencialmente uma solicitação por força, o módulo de segurança encaminha a força para os circuitos essenciais até que um sinal do BIOS, ou um período de intervalo expira, antes de encaminhar a força para outros circuitos, tal como um teclado ou interface de mouse.

A compactação do módulo de segurança e do processador do sistema em um módulo de múltiplos circuitos integrados, ou híbrido similar, ajuda a garantir que o módulo de segurança não seja simplesmente desativado por um ataque de "corte e ponte" (cut and jumper) nas linhas de força. Em uma modalidade, o processador do sistema usa uma arquitetura que integra as funções "Northbridge" tradicionais de gerenciamento de memória. Isso permite que uma função adicional do módulo de segurança seja implementada para monitorar a atividade do barramento. Especialmente quando o processador usa um barramento orientado a pacotes, tal como um barramento Hypertransport™, o módulo de segurança pode monitorar o tráfego para determinar se tráfego não autorizado está ocorrendo e adotar uma ação apropriada, tal como reinicializar o computador. O módulo de segurança pode também fazer com que o barramento reinicialize periodicamente, para impor o limite de memória reduzido. Em uma modalidade, a função de monitor do barramento do módulo de segurança pode ser capaz de desativar linhas individuais no barramento, para impor tamanho de memória reduzido.

Quando a operação do computador é projetada para uso normal medido, o módulo de segurança pode suprir o BIOS normal. Durante a operação normal, o módulo de segurança, usando uma função criptográfica embutida, pode gerenciar a medição ou assinaturas, incluindo os processos associados com a adição de valor, tempo ou assinaturas no computador.

## BREVE DESCRIÇÃO DOS DESENHOS

A figura 1 é um diagrama de blocos de uma vista a lógica de um computador.

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

A figura 3 é um diagrama de blocos simplificado e representativo de um módulo de segurança e

A figura 4 é um fluxograma representando um método exemplar de imposição de um modo de operação de função limitada em um computador.

DESCRIÇÃO DETALHADA

Embora o texto seguinte apresente uma descrição detalhada de numerosas modalidades diferentes, deve ser entendido que o escopo legal da descrição é definido pelas palavras das reivindicações apresentadas no fim dessa revelação. A descrição detalhada deve ser interpretada como exemplar somente e não descreve cada modalidade possível desde que descrever cada modalidade possível não seria prático, se não impossível. Numerosas modalidades alternativas poderiam ser implementadas usando a tecnologia corrente ou a tecnologia desenvolvida depois da data de depósito dessa patente, que ainda se situaria dentro do escopo das reivindicações.

Também deve ser entendido que, a menos que um termo seja expressamente definido nessa patente usando a frase "Como usado aqui, o termo '_____' é dessa maneira definido para significar_____" ou uma frase similar, não existe intenção de limitar o significado desse termo, tanto expressamente quanto por implicação, além do seu significado simples ou comum, e tal termo não deve ser interpretado para ser limitado no escopo com base em qualquer declaração feita em qualquer seção dessa patente (diferente da linguagem das reivindicações). Até a extensão que qualquer termo recitado nas reivindicações no fim dessa patente é citado nessa patente em uma maneira consistente com um significado único, isso é feito com o intuito de clareza somente de modo a não confundir o leitor e não é planejado que tal termo de reivindicação seja limitado, por implicação ou de outra forma, a esse significado único. Finalmente, a menos que um elemento de reivindicação seja definido receitando a palavra "significa" e uma função sem a exposição de qualquer estrutura, não é planejado que o escopo de qualquer elemento de reivindicação seja interpretado com base na aplicação de 35 U.S.C. § 112, sexto parágrafo.

Muita da funcionalidade inventiva e muitos dos princípios inventivos são implementados melhor com ou em programas de software ou instruções e circuitos integrados (ICs) tal como ICs específicos da aplicação. É esperado que alguém versado, não obstante um esforço possivelmente significativo e muitas escolhas de projeto motivadas por, por exemplo, tempo disponível, tecnologia corrente e considerações econômicas, quando guiado pelos conceitos e princípios revelados aqui, seja prontamente capaz de gerar tais instruções de software e programas e ICs com mínima experimentação. Portanto, no interesse de bre-

vidade e minimização de qualquer risco de obscurecer os princípios e os conceitos de acordo com a presente invenção, discussão adicional de tal software e ICs, se alguma, será limitada aos elementos essenciais com relação aos princípios e conceitos das modalidades preferidas.

Muitos computadores de alto valor da técnica anterior, assistentes digitais pessoais, organizadores e assim por diante não são adequados para uso em um modelo de negócios de pré-pagamento ou pagamento por uso como se encontram. A capacidade de impor um contrato exige que um provedor de serviço, ou outra entidade de imposição, seja capaz de afetar a operação de um dispositivo mesmo embora o dispositivo possa não estar conectado no provedor de serviço, por exemplo, conectado na Internet. Um primeiro estágio da imposição pode incluir um aviso instantâneo simples, indicando que os termos do contrato estão próximos de um ponto crítico. Um segundo estágio da imposição, por exemplo, depois que os minutos de pagamento por uso expiraram ou um período de assinatura decorreu, pode ser apresentar uma interface de usuário modal do sistema para adicionar valor e restaurar o serviço. O poder final de um provedor para impor os termos de um acordo de assinatura ou de pagamento quando você usa é desativar o dispositivo. Uma tal etapa dramática pode ser apropriada quando aparenta que o usuário fez uma tentativa deliberada de subverter a medição ou outros sistemas de segurança ativos no dispositivo.

Usos para a capacidade de colocar um dispositivo eletrônico em um modo de função limitada podem se estender além das aplicações de assinatura e pagamento por uso. Por exemplo, técnicas para consumo de capacidade poderiam ser usadas para licenciar a imposição de um sistema operacional ou aplicações individuais.

A figura 1 ilustra uma vista lógica de um dispositivo de computação na forma de um computador 110 que pode ser usado em um modo de assinatura ou pagamento por uso. Com o intuito de ilustração, o computador 110 é usado para ilustrar os princípios da revelação instantânea. Entretanto, tais princípios se aplicam igualmente a outros dispositivos eletrônicos incluindo, mas não limitados a, telefones celulares, assistentes digitais pessoais, reprodutores de mídia, equipamentos, sistemas de jogos, sistemas de entretenimento, conversores de frequência, eletrônica de painel de automóvel, para citar alguns. Componentes do computador 110 podem incluir, mas não são limitados a uma unidade de processamento 120, uma memória do sistema 130 e um barramento do sistema 121 que acopla vários componentes do sistema incluindo a memória do sistema na unidade de processamento 120. O barramento do sistema 121 pode ser qualquer um de vários 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. Por meio de exemplo, e não limitação, tais arquiteturas incluem barramento Industry Standard Architecture (ISA), barramento Micro Channel Architecture (MCA), barra-

mento Enhanced ISA (EISA), barramento local Video Electronics Standards Association (VESA) e barramento Peripheral Component Interconnect (PCI), barramento de lado frontal e barramento Hypertransport ™, um barramento de largura variável usando um protocolo de dados em pacote.

O computador 110 pode incluir um módulo de segurança 125 (SM). O SM 125 pode ser habilitado para executar o monitoramento de segurança, gerenciamento de uso de assinatura e pagamento por uso e a imposição da diretriz relacionada com os termos e condições associados com o uso pago, particularmente em um modelo de negócios de compra subsidiada. O módulo de segurança 125 pode ser personificado na unidade de processamento 120, como um componente independente, ou um híbrido, como representado nas figuras posteriores.

O computador 110 tipicamente inclui uma variedade de meios legíveis por computador. Meios legíveis por computador podem ser quaisquer meios disponíveis que possam ser acessados pelo computador 110 e incluem ambos meios voláteis e não voláteis, meios removíveis e não removíveis. Por meio de exemplo, e não limitação, meios legíveis por computador podem compreender meios de armazenamento no computador e meios de comunicação. Meios de armazenamento no computador incluem meios voláteis e não voláteis, removíveis e não removíveis implementados em qualquer método ou tecnologia para armazenamento de informação, tais como instruções legíveis por computador, estruturas de dados, módulos do programa ou outros dados. Meios de armazenamento no computador incluem, mas não são limitados a, 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 outro meio que possa ser usado para armazenar a informação desejada e que possa ser acessado pelo computador 110.

A memória do sistema 130 inclui meios de armazenamento no computador na forma de memória volátil e/ou não volátil, tais como memória somente de leitura (ROM) 131 e memória de acesso aleatório (RAM) 132. Um sistema básico de entrada/saída 133 (BIOS), 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 ficam imediatamente acessíveis para e/ou atualmente sendo operados pela unidade de processamento 120. Por meio de exemplo e não limitação, a figura 1 ilustra o sistema operacional 134, programas de aplicação 135, outros módulos de programa 136 e dados de programa 137.

O computador 110 pode também incluir outros meios de armazenamento no computador removíveis/não removíveis, voláteis/não voláteis. Por meio de exemplo somente, a figura 1 ilustra uma unidade de disco rígido 140 que lê de ou escreve em meios magnéticos

não removíveis, não voláteis, uma unidade de disco magnético 151 que lê de ou escreve em um disco magnético removível, não volátil 152 e uma unidade de disco ótico 155 que lê de ou escreve em um disco ótico removível, não volátil 156, tal como um CD-ROM ou outros meios óticos. Outros meios de armazenamento no computador removíveis/não removíveis, voláteis/não voláteis que podem ser usados no ambiente de operação exemplar incluem, mas não são limitados a, cassetes de fita magnética, placas de memória flash, discos versáteis digitais, fita de vídeo digital, RAM do estado sólido, ROM do estado sólido e semelhantes. A unidade de disco rígido 141 é tipicamente conectada no barramento do sistema 121 através 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 no barramento do sistema 121 por uma interface de memória removível, tal como interface 150.

As unidades e seus meios de armazenamento no computador associados, discutidos acima e ilustrados na figura 1, proporcionam armazenamento de instruções legíveis por computador, estruturas de dados, módulos do programa e outros dados para o computador 110. Na figura 1, por exemplo, a unidade de disco rígido 141 é ilustrada como armazenando o sistema operacional 144, programas de aplicação 145, outros módulos do programa 146 e dados do programa 147. Observe que esses componentes podem ser os mesmos que ou diferentes do sistema operacional 134, programas de aplicação 135, outros módulos de programa 136 e dados do programa 137. O sistema operacional 144, programas de aplicação 145, outros módulos do programa 146 e dados do programa 147 são fornecidos com números diferentes aqui para ilustrar que, no mínimo, eles são cópias diferentes. Um usuário pode inserir comandos e informação no computador 20 através de dispositivos de entrada, tais como um teclado 162 e dispositivo indicador 161, geralmente citado como um mouse, trackball ou mesa sensível ao toque. Outros dispositivos de entrada (não mostrados) podem incluir um microfone, barra de direção, mesa de jogos, disco de satélite, scanner, câmera digital ou assim por diante. Esses e outros dispositivos de entrada são frequentemente conectados na unidade de processamento 120 através de uma interface de entrada do usuário 160 que é acoplada no barramento do sistema, mas pode ser conectada 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 é também conectado no barramento do sistema 121 através de uma interface, tal como uma interface de vídeo 190.

O computador 110 pode operar em um ambiente de rede usando conexões lógicas para um ou mais computadores remotos (não representados) através de uma interface de rede 170, tal como a conexão da Ethernet de banda larga ou outra rede conhecida.

A figura 2 é um diagrama arquitetônico de um computador 200, o mesmo que ou similar ao computador da figura 1. O computador 200 pode incluir um processador 204. O

processador 204 pode também incluir um gerenciador de memória, a assim chamada função "Northbridge". Tais processadores estão disponíveis de Advanced Micro Devices e outros. Um módulo de segurança 206 pode incluir memória segura, funções criptográficas e outras funções especializadas. O módulo de segurança é discutido em mais detalhes abaixo. O processador 204 e o módulo de segurança 206 podem ser acondicionados em um primeiro circuito 208 como um módulo de múltiplos circuitos integrados (MCM) ou juntos em uma placa filha. O acondicionamento mecânico desse tipo pode melhorar a segurança geral da combinação tornando a combinação mais difícil de piratear a partir de uma perspectiva de hardware, por exemplo, um ataque de "corte e ponte" de rastreio ou remoção de circuito integrado com substituições de "falha morta".

Um abastecimento de força 210 pode incluir uma saída de controle 211, também conhecida como um "força OK" usada para sinalizar que a saída do abastecimento de força está na voltagem e estável. Um tal sinal é frequentemente usado como uma entrada em circuitos integrados grandes ou de alto valor para protegê-los da baixa voltagem ou força instável que pode afetar o desempenho do circuito ou causar danos. A saída de controle 211 pode passar através do módulo de segurança 206 via a linha de sinal 212 para refrear temporariamente a inicialização dos dispositivos de circuito não principais 208, como descrito abaixo.

Um barramento de dados 214 pode ser uma disposição de barramento convencional com linhas de dados bidirecionais. O barramento de dados 214 pode também ser um barramento unidirecional de ponto a ponto, tal como um barramento Hypertransport™. Um tal barramento pode suportar dados de pacote, ao invés dos dados sincronizados de um barramento mais convencional. Para suportar dados bidirecionais, um barramento de dados desse tipo pode, na realidade, ter uma segunda conexão de dados de trajetória inversa. Os barramentos unidirecionais de ponto a ponto podem ser conectados em série para conectar dispositivos adicionais. Na figura 2, o módulo de segurança 206 é mostrado frouxamente acoplado no barramento de dados 214, mas pode na realidade ser simplesmente um outro dispositivo na corrente margarida.

Um controlador de I/O, ou Southbridge 216, pode ser usado para conectar na memória do sistema 218 ou dispositivos periféricos tal como fendas de placa 222, conexões de rede remota ou local 224, ou memória não volátil 226, por exemplo, memória flash ou um disco rígido, tal como disco rígido 141 da figura 1. Um outro controlador de I/O, ou Super I/O 228, pode também ser usado para conectar menos dispositivos de dados intensivos ou não endereçáveis, tal como um mouse/teclado 230, I/O serial e paralelo 232 e uma chave de "ligar" 234.

Em operação, quando a chave de ligar 234 é apertada, um sinal é enviado do super I/O 228 no modo de prontidão para o módulo de segurança 206 usando a linha do sinal 213,

indicando uma solicitação para energizar o computador 200. O abastecimento de força 210 pode ser alternado de prontidão para força total. O abastecimento de força 210 pode sinalizar o módulo de segurança 206 usando a saída de controle 211 que a força total está disponível e estável. Entretanto, o módulo de segurança 206 pode manter um estado desativado na saída de controle 212 para o super I/O 228, mantendo os componentes do computador fora do primeiro circuito 208 em reinicialização. Muitos outros métodos de gerenciamento de uma sequência de partida além da manipulação dos sinais de força OK podem ser usados nesse contexto. Em uma modalidade, a força real pode ser alternada no módulo de segurança 206 para o super I/O 228 ou para outros componentes críticos do sistema. Em ainda uma outra modalidade, os sinais codificados podem ser usados para permitir que o módulo de segurança restrinja a operação dos componentes selecionados fora do primeiro circuito 208 até que a configuração de segurança no primeiro circuito 208 está completa.

Depois que o módulo de segurança 206 e o processador 204 têm força e começam o ciclo de inicialização, um BIOS pode ser suprido pelo módulo de segurança 206 para o processador para operação inicial do computador 200. O módulo de segurança 206 pode também usar a sua conexão no barramento de dados 214 para bloquear o tráfego de dados durante a fase de inicialização inicial, primariamente para tornar mais difícil para um pirata acessar o processador quando o BIOS está carregando e começando. O BIOS suprido para o processador 204 pode ser uma função dos dados armazenados no módulo de segurança 206 indicando se o computador 200 deve inicializar em um modo de operação ou um modo de função reduzida. O processador 204 configurará o barramento de dados 214 de acordo com as instruções no BIOS selecionado, isto é, acesso de memória total para o modo operacional ou acesso de memória limitado para o modo de função reduzida. Parte da partida do BIOS pode ser para ler um registrador no módulo de segurança 206 para verificar o estado (operacional ou restrito) do computador 200. Se o BIOS errado é carregado, isto é, um BIOS de operação total, quando o registrador é ajustado para restrito, o BIOS de operação total pode simplesmente parar. Isso ajudará a impedir um ataque de substituição do BIOS, isto é, quando um BIOS no módulo de segurança 206 é usado no lugar do outro.

Quando o BIOS tiver alcançado um ponto onde o barramento de dados é configurado e quaisquer programas iniciais estão estáveis, o módulo de segurança pode desbloquear o barramento de dados 214 e suprir o sinal de força OK na saída de controle 212. Quando o módulo de segurança 206 mantém o barramento de dados 214 bloqueado até sinalizado pelo BIOS, um ataque de substituição de BIOS potencial (usando um novo BIOS externo) é impedido, porque o protocolo de BIOS para módulo de segurança 206 para desbloquear o barramento de dados 214 terá que ser projetado invertido antes que o BIOS de substituição seja capaz de desbloquear o barramento de dados. Quando o sinal de força OK é detectado no circuito integrado super I/O 228, o resto do circuito integrado super I/O é ha-

bilitado e o restante do computador 200 é capaz de avançar para um estado operacional.

O BIOS ajusta o estado do computador 200, notavelmente, a quantidade de memória do sistema 218 disponível para o processador 204. Na maior parte dos casos, o BIOS pode executar uma inquisição quanto ao tamanho da memória e ajustar os limites da memória de acordo. Entretanto, no caso da operação restrita, o BIOS pode simplesmente ajustar a memória para um dado tamanho, a despeito da disponibilidade de mais memória. Em uma modalidade, o tamanho da memória é ajustado para acomodar uma rotina de BIOS que manipula a entrada do usuário para interação com o módulo de segurança para restaurar um estado operacional. Em uma outra modalidade, o tamanho da memória é ajustado para 4 megabytes. Isso é menos do que 1% da memória do sistema de 1 gigabyte comum em sistemas atuais e bem menos do que a quantidade requerida para carregar e executar qualquer sistema operacional atual, jogo ou aplicação de escritório.

O módulo de segurança 206 pode usar o seu acesso ao barramento de dados 214 para várias finalidades depois da inicialização. O módulo de segurança 206 pode simplesmente monitorar o barramento de dados para ver que a faixa de endereço correta está sendo usada. Se os endereços caem fora da faixa válida, o módulo de segurança 206 pode puxar a linha de força OK 212 e o computador 200 reinicializará. O módulo de segurança 206 pode também monitorar o tráfego atual no barramento de dados 214, analisando as instruções e os valores de dados já identificados como pertencentes a um ataque conhecido (uma impressão digital do ataque) ou simplesmente envolvendo instruções e valores de dados inesperados. Novamente, o resultado de mau comportamento conhecido ou suspeito pode ser uma reinicialização do sistema. O monitoramento nesse modo é simplificado quando o barramento de dados 214 é um barramento de dados orientado a pacotes encaminhado através do módulo de segurança 206, porém dados convencionais e operações de barramento de endereço podem ser similarmente monitorados. Para bloquear o barramento de dados 214, como durante a partida, o módulo de segurança 214 pode não retransmitir os dados em um barramento de dados de corrente margarida de ponto a ponto, ou pode carregar as linhas de dados de um barramento convencional para o ponto em que os dados fiquem ilegíveis.

Durante a operação restrita, uma aplicação mínima pode funcionar a partir do BIOS de operação restrita. Entrada de teclado e somente gráficos de pequena resolução podem ser suportados, permitindo que um usuário ou pessoa de serviço do consumidor entre um código para adicionar valor ou restaurar o estado da assinatura para o computador 200. Quando o código tiver sido inserido e verificado, o módulo de segurança 206 pode reavaliar os contadores apropriados associados com a operação medida normal. O módulo de segurança 206 pode também reinicializar o indicador de inicialização para operação restrita, de modo que o próximo ciclo de inicialização resultará em operação normal medida. O módulo

de segurança 206 pode automaticamente reinicializar o sistema depois que o indicador foi assim ajustado.

A figura 3 é um diagrama de blocos simplificado e representativo de um módulo de segurança 300. O módulo de segurança 300 pode incluir um processador 302 e uma memória 304 incluindo um primeiro BIOS 306 e um segundo BIOS 308. A memória 304 pode incluir ambas as memórias volátil e não volátil. Pelo menos a porção da memória armazenando o primeiro e o segundo BIOS 306 308 é preferivelmente memória segura e exige autenticação criptográfica antes que ela possa ser alterada. Uma outra porção da memória 304 pode ser usada como arquivo temporário pelo processador 302. O processador pode ser um processador ARM® Core ou um controlador de circuito integrado único de companhias tais como Intel, SST ou Freescale.

Um supervisor de barramento 310 pode incluir um registrador 312 para armazenar um indicador de inicialização, descrito acima. Um circuito de controle de força 314 pode incluir uma entrada de força OK 316 e uma saída de força OK 318. A entrada de força OK 316 pode ser usada para gerenciar a força interna dos dispositivos do módulo de segurança e também como um sinal que a saída de força OK 318 pode ser ajustada depois da autorização do processador 302. O processamento do sinal de força OK pode ser realizado usando um circuito independente no módulo de segurança 300 ou pode ser implementado em software usando entradas analógicas ou digitais no processador 302, dependendo da conveniência e disponibilidade de I/O. Um módulo criptográfico 320 pode ser usado para gerenciar os dados de medição/assinatura, bem como para qualificar os processos de adição de valor e restauração. O módulo criptográfico 320 pode ser um circuito integrado inteligente, tal como um Infineon SLE66, ou pode ser implementado em software no processador.

O supervisor de barramento 310 pode ser acoplado em um barramento de dados 324 tendo linhas de dados individuais 326 e pode ser a conexão entre um processador de computador 328 e um circuito de interface de memória, tal como Southbridge 330. Como discutido acima, o supervisor de barramento 310 pode servir para monitorar o tráfego no barramento 324, bloquear todo o barramento 324, bloquear linhas de dados individuais, ou todos, dependendo da implementação. Pelo fato de que o supervisor de barramento 310 é um participante do barramento de dados total, as facilidades do módulo de segurança 300 podem ficar disponíveis para o processador 328. Por exemplo, enquanto inicializando, o supervisor de barramento 310 pode ser usado para suprir o BIOS selecionado para o processador de computador 328. Quando no modo de operação restrita, o supervisor de barramento 310, sob o controle do processador 302, pode executar um ciclo de configuração no barramento de dados para garantir que o barramento seja ajustado para o tamanho de memória limitado, por exemplo, 4 megabytes. Também, pelo fato de que o processador 302 pode se comunicar com o Southbridge 330 e o processador do computador 328, o proces-

sador pode consultar o sistema para determinar o tamanho da memória configurada. Como acima, se o tamanho da memória configurada não iguala o tamanho esperado da memória configurada, o processador pode causar uma reinicialização do sistema. Mesmo se o módulo de segurança 300 não pode impedir o uso desautorizado, o módulo de segurança 300 tem vários recursos à sua disposição para tornar o uso desautorizado menos produtivo.

O módulo de segurança 300 pode ser um módulo de múltiplos circuitos integrados (MCM) e pode tirar vantagem das linhas de sinal enterradas, planos de força e técnicas de montagem mecânicas para ajudar a limitar os ataques de hardware limitando o acesso às trajetórias de sinal críticas, tal como uma linha de reinicialização do processador do computador (não representada) que pode ser usada em conjunto com a linha de força OK para causar uma reinicialização. As capacidades de integração futuras certamente permitirão que os circuitos e funções descritos aqui como separados ou em um MCM sejam integrados em um circuito único. Pode ser esperado que em algum ponto razoavelmente perto, todas essas funções fiquem disponíveis em um único circuito integrado junto com o processador do computador 328.

O circuito de controle de força 314 pode ficar em comunicação bidirecional com o processador 302, tanto alertando o processador 302 quando a entrada de força OK 316 está ativa (geralmente alta) quanto quando mudar a saída de força OK 318 para ativa. Quando o processador 302 determina que uma reinicialização do sistema é apropriada, ele pode passar a saída de força OK 318 para inativa, dessa maneira causando uma reinicialização. Para ajudar a impedir um ataque de corte e ponte na saída de força OK 318, o processador 302 pode também fazer com que o processador do computador 328 reinicialize, usando uma conexão de sinal local ao MCM (não representado) e não facilmente acessível sem danos aos componentes circundantes.

A figura 4 é um fluxograma representando um método exemplar 400 de imposição de um modo de operação de função limitada em um computador 200. No bloco de partida 402, um computador 200 pode começar um ciclo de reinicialização. Um abastecimento de força 210 pode mudar um sinal de força OK 211 indicando que o abastecimento de força 210 está estável. No bloco 404, um sensor em um primeiro circuito 208 pode ler o sinal de força OK 211 e começar um processo de partida para o primeiro circuito 208, que pode incluir um processador 204 e um módulo de segurança 206. No bloco 406, uma colocação salva antes do ciclo de inicialização atual pode ser lida para determinar se o computador 200 deve ser operado em um modo medido de uso total ou deve ser operado em um modo restrito, indicativo de um pequeno valor para tempo de uso pré-pago ou uma assinatura expirada. O BIOS selecionado pode ser carregado no bloco 408 e executado. Como parte do processo de partida, no bloco 410, o BIOS ajustará a quantidade de memória disponível para o processador 204. No bloco 412, quando o módulo de segurança 206 tiver determina-

do que o BIOS selecionado completou a alocação da memória, um sinal de força OK 212, ou força do sistema, pode ser habilitado para as porções restantes do computador 200. No bloco 414, um componente do supervisor de barramento do módulo de segurança 206 pode monitorar o tráfego sobre um barramento de dados 214, periodicamente verificar que a memória disponível iguala uma colocação apropriada para o BIOS selecionado ou ambos. Quando o tráfego e o tamanho da memória satisfazem critérios apropriados, a linha sim do bloco 414 pode ser adotada e o processo de verificação repetido em uma base periódica. Um de, no bloco 414, tráfego ou tamanho de memória não satisfaz os critérios apropriados, a linha não do bloco 414 pode ser adotada para o bloco 416. No bloco 416, o módulo de segurança 206 pode causar uma reinicialização do sistema que retornará a operação para o bloco 402.

A capacidade de selecionar um BIOS com base em uma colocação prévia e permitir que um módulo de segurança monitore a configuração do barramento de dados gerenciando o tráfego do processador para a memória provê um conjunto de ferramenta efetiva para gerenciar um computador de assinatura ou uso do papel, ou outro dispositivo eletrônico. O sistema de verificações e balanços incluindo o BIOS verificando um indicador de inicialização, o módulo de segurança verificando a configuração do sistema e o módulo de segurança usando um monitor de barramento para criar a impressão digital do tráfego do processador cria um nível de segurança previamente indisponível para gerenciar um bem remoto. A capacidade de desativar um computador remoto quando os termos de uma compra de pagamento pelo uso ou assinatura não são honrados permite ao sistema e provedores de serviço uma ferramenta poderosa para proteger os seus bens. Ao mesmo tempo, o módulo de segurança é a única adição em um sistema de outra forma preenchido com componentes prontos, disponíveis na indústria.

Embora o texto precedente apresente uma descrição detalhada de numerosas modalidades diferentes da invenção, deve ser entendido que o escopo da invenção é definido pelas palavras das reivindicações apresentadas no fim dessa patente. A descrição detalhada deve ser interpretada como exemplar somente e não descreve cada modalidade possível da invenção porque descrever cada modalidade possível não seria prático, se não impossível. Numerosas modalidades alternativas poderiam ser implementadas usando a tecnologia corrente ou a tecnologia desenvolvida depois da data de depósito dessa patente, que ainda se situaria dentro do escopo das reivindicações que definem a invenção.

Dessa maneira, muitas modificações e variações podem ser feitas nas técnicas e estruturas descritas e ilustradas aqui sem se afastar do espírito e do escopo da presente invenção. Dessa forma, deve ser entendido que os métodos e aparelho descritos aqui são ilustrativos somente e não estão limitando o escopo da invenção.

## REIVINDICAÇÕES

1. Módulo disposto em um computador de uso medido para imposição da operação do computador de uso medido em um modo de uso restrito, o módulo **CARACTERIZADO** pelo fato de que compreende:

um processador,

uma memória acoplada no processador armazenando código executável e colocações,

um supervisor de barramento acoplado no processador e preso em um barramento do sistema acoplando um processador do computador e uma memória do computador, o supervisor de barramento operável para possibilitar o tráfego no barramento do sistema responsivo a um primeiro sinal do processador,

uma função criptográfica disponível para o processador e

um circuito de controle de força que retarda o começo de uma porção do computador de uso medido responsivo a um segundo sinal do processador.

2. Módulo, de acordo com a reivindicação 1, **CARACTERIZADO** pelo fato de que a função criptográfica é um circuito integrado inteligente.

3. Módulo, de acordo com a reivindicação 1, **CARACTERIZADO** pelo fato de que a função criptográfica é software executando no processador.

4. Módulo, de acordo com a reivindicação 1, **CARACTERIZADO** pelo fato de que o barramento do sistema é um barramento de dados de alta velocidade orientado a pacotes.

5. Módulo, de acordo com a reivindicação 1, **CARACTERIZADO** pelo fato de que o supervisor de barramento compreende um registrador do modo de inicialização.

6. Módulo, de acordo com a reivindicação 1, **CARACTERIZADO** pelo fato de que o comportamento predefinido do supervisor de barramento é desativar o tráfego no barramento do sistema até a recepção do primeiro sinal.

7. Módulo, de acordo com a reivindicação 1, **CARACTERIZADO** pelo fato de que o supervisor de barramento é também operável para monitorar o tráfego no barramento do sistema para tráfego de dados desautorizado durante a operação de uso restrito.

8. Módulo, de acordo com a reivindicação 1, **CARACTERIZADO** pelo fato de que o processador periodicamente reinicializa o barramento do sistema para tamanho de memória restrito durante a operação de uso restrito.

9. Método de operação de um computador em um modo restrito, **CARACTERIZADO** pelo fato de que compreende:

iniciar um ciclo de inicialização no computador,

energizar um primeiro circuito que controla um sinal de força para um dispositivo de interface,

selecionar um BIOS a partir de um conjunto de BIOSs armazenado no primeiro cir-

cuito, de acordo com uma colocação salva antes do ciclo de inicialização,

executar o BIOS selecionado,

possibilitar uma mudança de barramento responsiva a um sinal gerado pelo BIOS selecionado para permitir o tráfego em um conjunto de trajetórias de dados associadas com um barramento do sistema depois que a operação do BIOS está estável,

verificar o estado do BIOS selecionado no primeiro circuito e

enviar um sinal de força para o dispositivo de interface.

10. Método, de acordo com a reivindicação 9, **CARACTERIZADO** pelo fato de que também compreende verificar a memória disponível para um processador do computador.

11. Método, de acordo com a reivindicação 9, **CARACTERIZADO** pelo fato de que também compreende executar uma aplicação de modo restrito do BIOS quando a colocação salva antes do ciclo de inicialização atual é indicativa de operação restrita.

12. Método, de acordo com a reivindicação 11, **CARACTERIZADO** pelo fato de que executar a aplicação do modo restrito no BIOS quando a colocação salva antes do ciclo de inicialização atual é indicativa de operação restrita compreende executar a aplicação de modo restrito para exibir um aviso e possibilitar a entrada do usuário para inserir um código de desbloqueio quando a colocação salva antes do ciclo de inicialização atual é indicativa da operação restrita.

13. Método, de acordo com a reivindicação 9, **CARACTERIZADO** pelo fato de que o primeiro circuito compreende o processador do computador, um processador local e a mudança do barramento.

14. Método, de acordo com a reivindicação 9, **CARACTERIZADO** pelo fato de que possibilitar uma mudança de barramento responsiva a um sinal compreende possibilitar a mudança do barramento para permitir o tráfego em um conjunto total das trajetórias de dados permitindo acesso a uma memória do sistema total quando usando um BIOS irrestrito e possibilitar a mudança do barramento para permitir o tráfego em um conjunto limitado de trajetórias de dados permitindo acesso a menos do que um por cento da memória do sistema total quando usando um BIOS de operação restrita.

15. Computador adaptado para operação medida tendo um modo medido e um modo restrito de operação, **CARACTERIZADO** pelo fato de que compreende:

um processador,

uma memória do sistema,

um conjunto de linhas de dados formando um barramento acoplando o processador na memória do sistema,

um conjunto de circuitos intermediários acoplando o processador nos dispositivos do sistema e periféricos e

um módulo de segurança tendo uma conexão de dados com o processador e cone-

xões de gerenciamento de força para o conjunto de circuitos intermediários, o módulo de segurança compreendendo:

um processador especializado,

uma memória local e

um monitor de barramento adaptado para seletivamente desativar o barramento e também adaptado para monitorar o tráfego de dados no barramento para uso de instrução não autorizado.

16. Computador, de acordo com a reivindicação 15, **CARACTERIZADO** pelo fato de que também compreende uma chave de ativação de força acoplada no módulo de segurança e o módulo de segurança também compreendendo um gerenciador de força responsivo a um sinal da chave de ativação de força para autorizar a força para pelo menos o módulo de segurança e o processador antes de autorizar a força para o conjunto de circuitos intermediários.

17. Computador, de acordo com a reivindicação 15, **CARACTERIZADO** pelo fato de que o módulo de segurança também compreende uma função criptográfica.

18. Computador, de acordo com a reivindicação 17, **CARACTERIZADO** pelo fato de que a função criptográfica é um entre um circuito integrado inteligente e um código executável implementando uma função criptográfica.

19. Computador, de acordo com a reivindicação 15, **CARACTERIZADO** pelo fato de que a memória local compreende código executável para um primeiro BIOS usado para inicializar o computador no modo medido e um segundo BIOS usado para inicializar o computador no modo restrito.

20. Computador, de acordo com a reivindicação 19, **CARACTERIZADO** pelo fato de que a memória local também compreende código executável como uma parte do segundo BIOS que, quando executado, faz com que o barramento monitore para desativar as linhas de dados individuais do conjunto de linhas de dados.

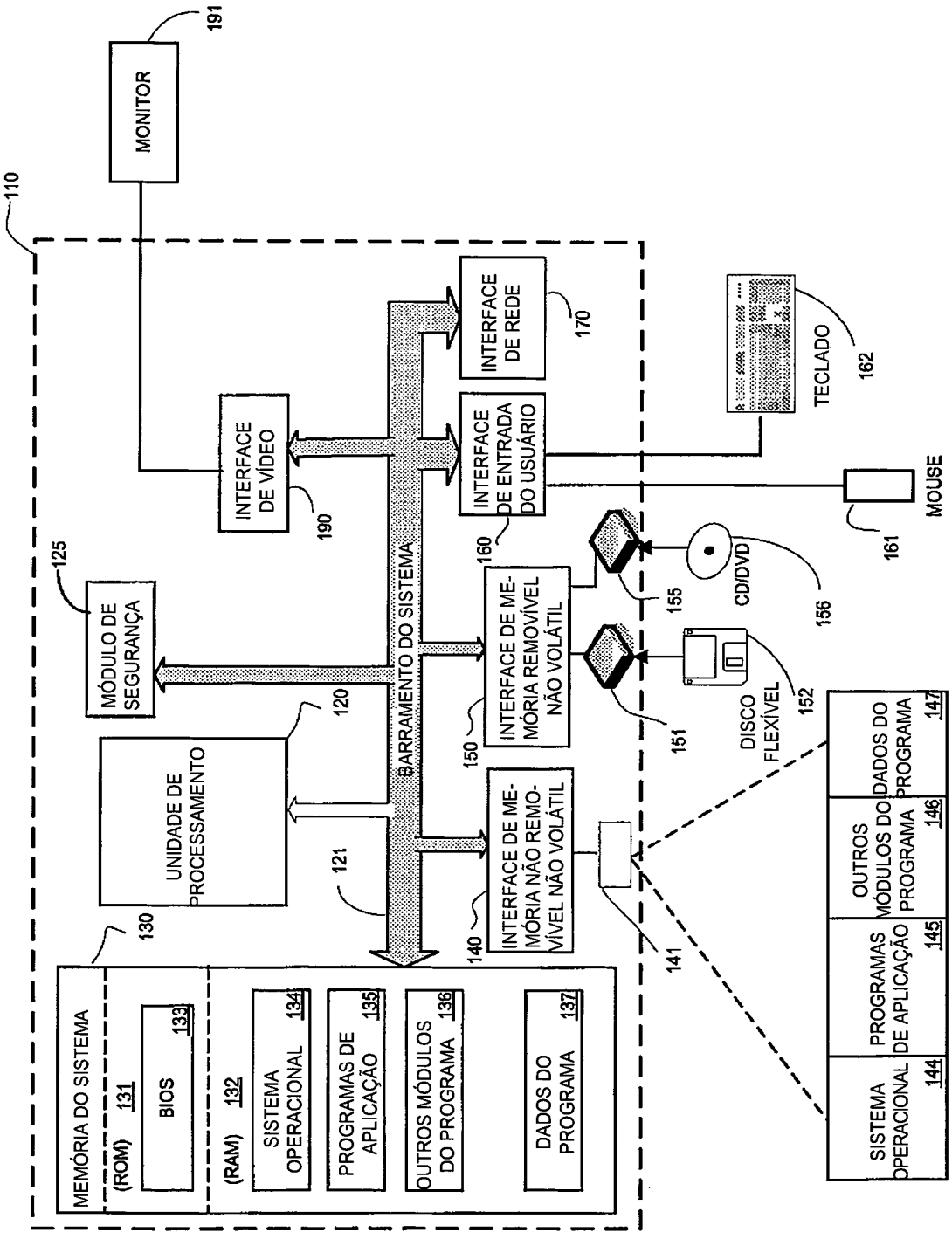

110
MONITOR
191
INTERFACE DE VÍDEO
190
INTERFACE DE REDE
170
INTERFACE DE ENTRADA DO USUÁRIO
160
TECLADO
162
MOUSE
161
125
MÓDULO DE SEGURANÇA
BARRAMENTO DO SISTEMA
120
UNIDADE DE PROCESSAMENTO
130
MEMÓRIA DO SISTEMA
(ROM) 131
BIOS 133
(RAM) 132
SISTEMA OPERACIONAL 134
PROGRAMAS DE APLICAÇÃO 135
OUTROS MÓDULOS DO PROGRAMA 136
DADOS DO PROGRAMA 137
INTERFACE DE MEMÓRIA REMOVÍVEL NÃO VOLÁTIL
150
INTERFACE DE MEMÓRIA NÃO REMOVÍVEL NÃO VOLÁTIL
140
121
141
155
CD/DVD
156
151
DISCO FLEXÍVEL
152
SISTEMA OPERACIONAL 144
PROGRAMAS DE APLICAÇÃO 145
OUTROS MÓDULOS DO PROGRAMA 146
DADOS DO PROGRAMA 147

Fig. 1

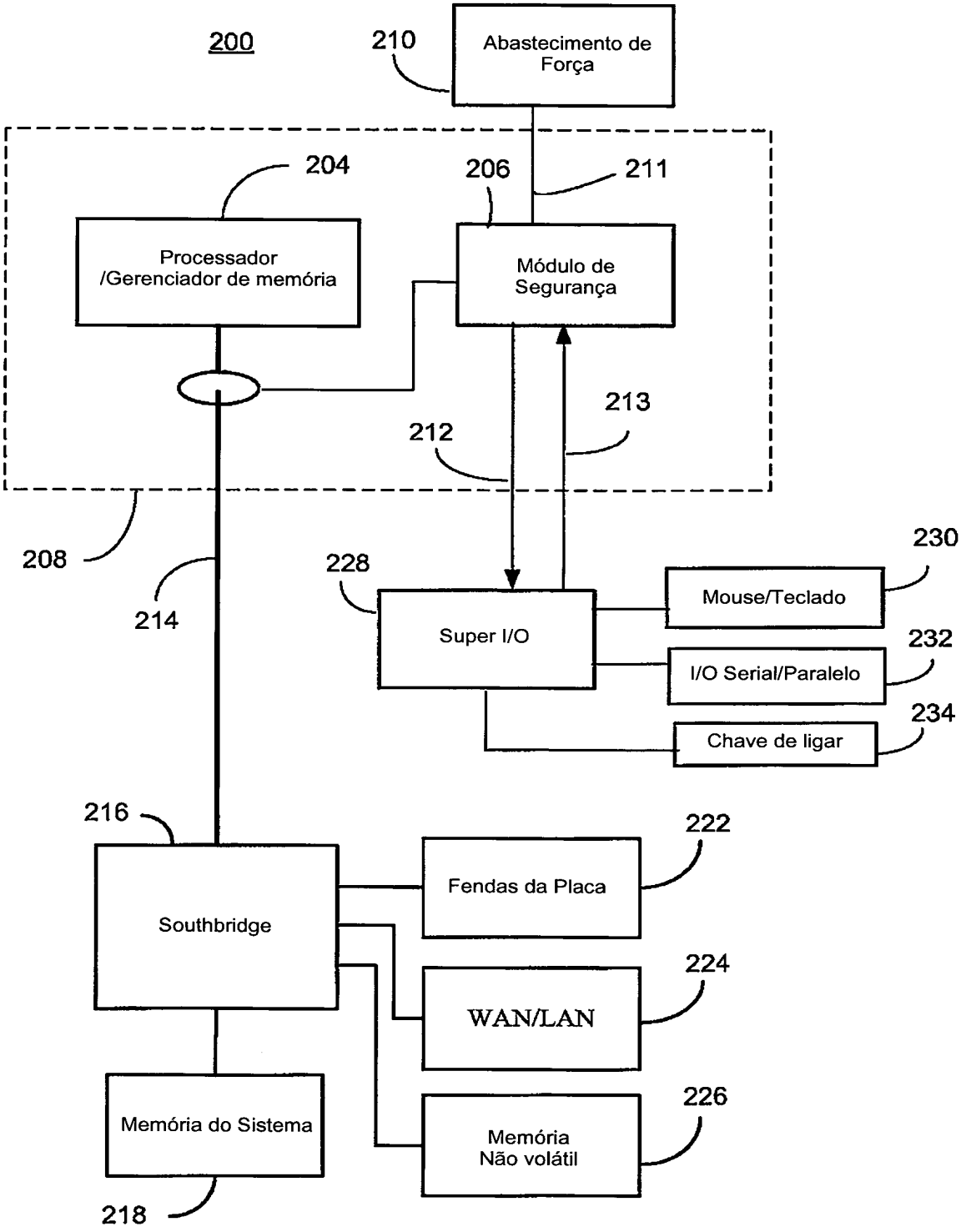

200
210
Abastecimento de Força
204
206
211
Processador /Gerenciador de memória
Módulo de Segurança
213
212
208
214
228
230
Mouse/Teclado
Super I/O
232
I/O Serial/Paralelo
234
Chave de ligar
216
222
Fendas da Placa
Southbridge
224
WAN/LAN
Memória do Sistema
226
Memória Não volátil
218

Fig. 2

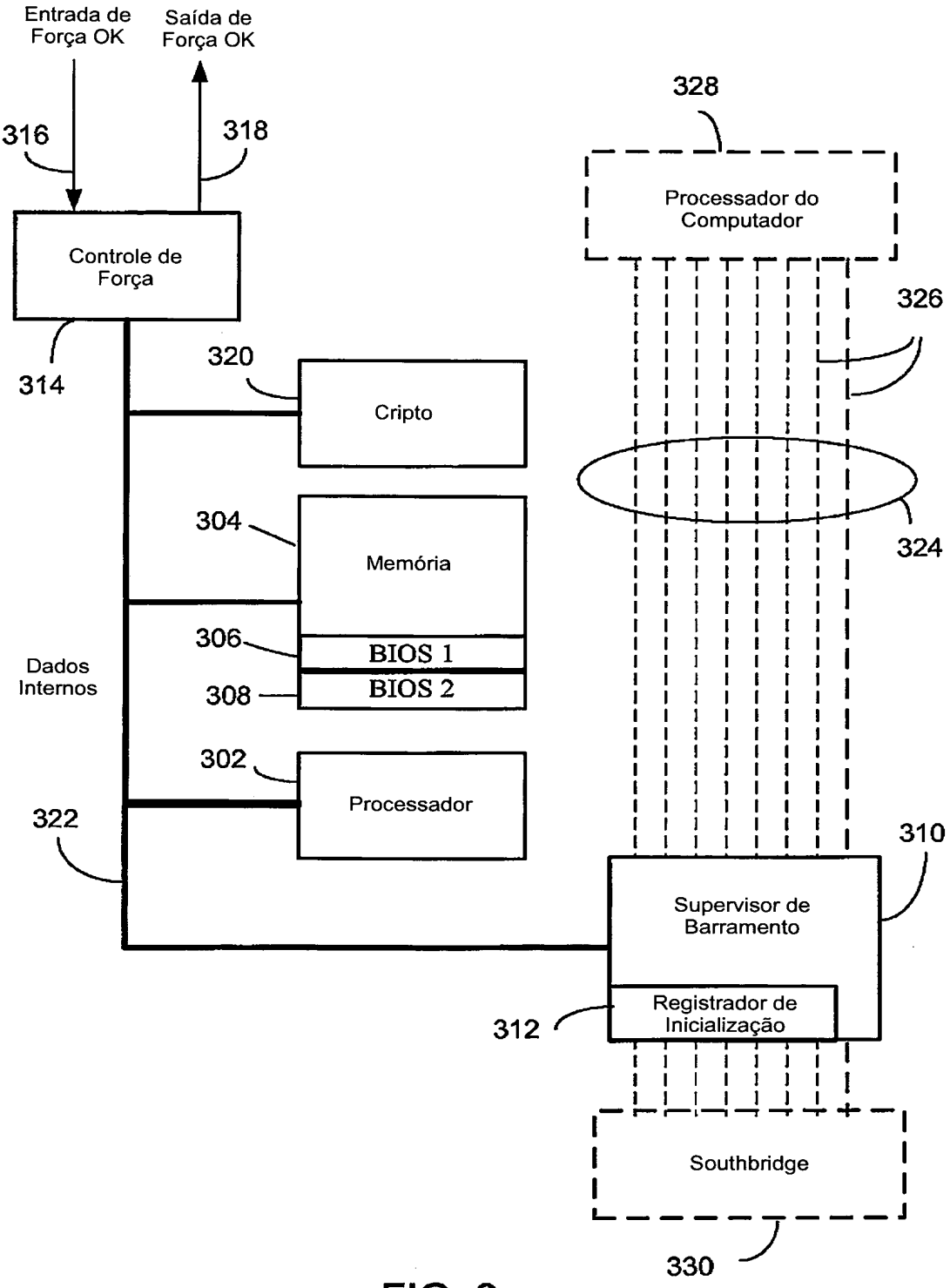

Entrada de Força OK
Saída de Força OK
316
318
328
Processador do Computador
Controle de Força
326
314
320
Cripto
304
Memória
324
306
BIOS 1
Dados Internos
308
BIOS 2
302
Processador
322
310
Supervisor de Barramento
Registrador de Inicialização
312
Southbridge
330

FIG. 3

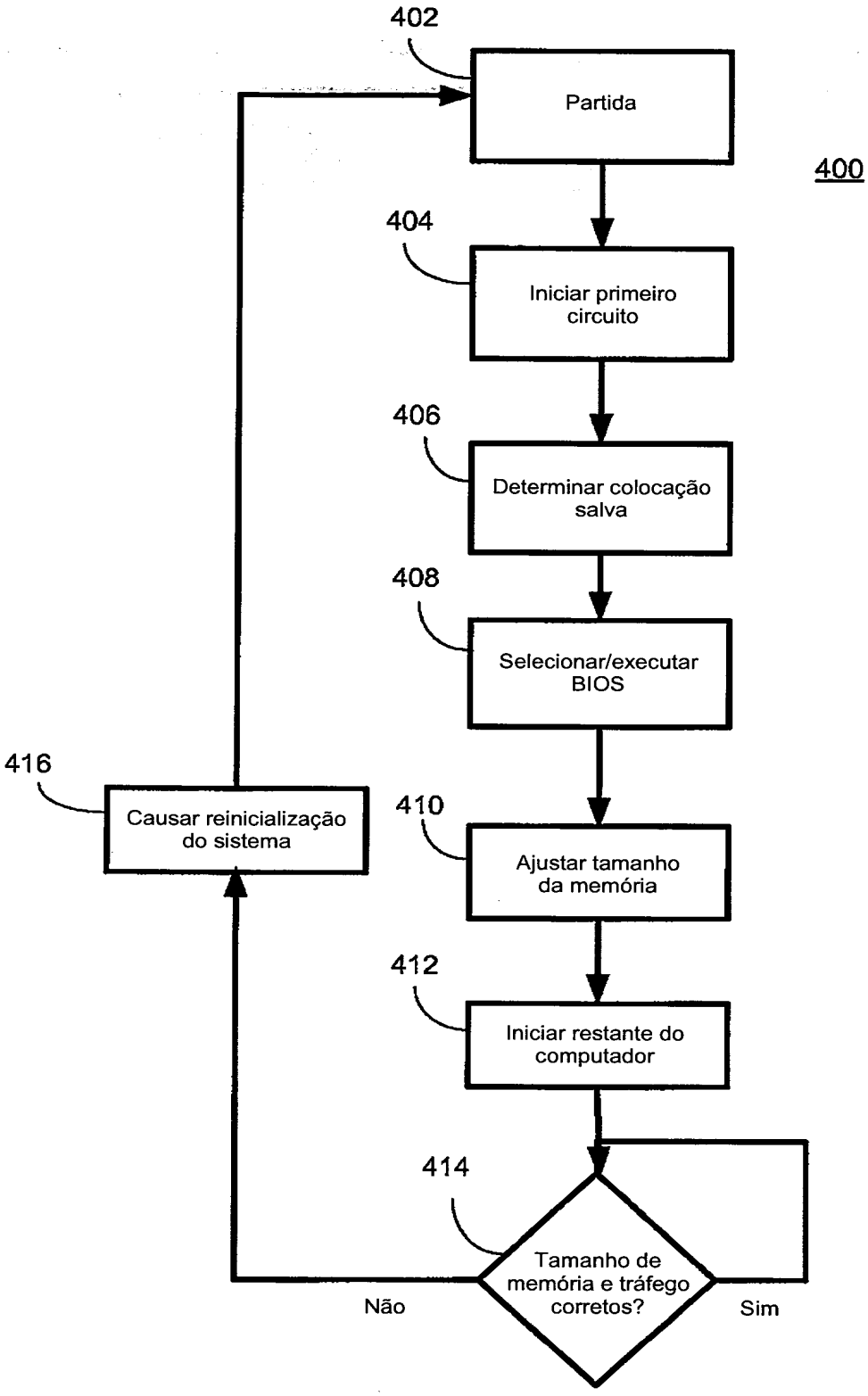

402
Partida
400
404
Iniciar primeiro circuito
406
Determinar colocação salva
408
Selecionar/executar BIOS
410
Ajustar tamanho da memória
412
Iniciar restante do computador
414
Tamanho de memória e tráfego corretos?
Não
Sim
416
Causar reinicialização do sistema

FIG. 4

## RESUMO

"IMPOSIÇÃO DE SUBMISSÃO NO COMPUTADOR"

Um módulo de segurança para um computador de pagamento por uso supre um BIOS apropriado para um dado modo de operação. Um gerenciador de força no módulo de segurança energiza somente os circuitos essenciais até que o BIOS esteja operacional para ajudar a impedir a substituição de um BIOS não autorizado. O módulo de segurança também inclui a capacidade de monitorar e restringir linhas de dados em um barramento entre um processador de computador principal e a memória do sistema de computador. Quando o computador está operando em um modo de uso restrito, as linhas de dados podem ser restritas para permitir somente acesso mínimo à memória do sistema de computador. Transações de barramento podem ser monitoradas para garantir que somente transações válidas fiquem ocorrendo e estejam dentro do espaço de memória projetado.