REPÚBLICA FEDERATIVA DO BRASIL
MINISTÉRIO DA INDÚSTRIA, COMÉRCIO EXTERIOR E SERVIÇOS
INSTITUTO NACIONAL DA PROPRIEDADE INDUSTRIAL

CARTA PATENTE Nº PI 0720921-5

O INSTITUTO NACIONAL DA PROPRIEDADE INDUSTRIAL concede a presente PATENTE DE INVENÇÃO, que outorga ao seu titular a propriedade da invenção caracterizada neste título, em todo o território nacional, garantindo os direitos dela decorrentes, previstos na legislação em vigor.

(21) Número do Depósito: PI 0720921-5

(22) Data do Depósito: 12/12/2007

(43) Data da Publicação do Pedido: 31/07/2008

(51) Classificação Internacional: G06F 9/06.

(30) Prioridade Unionista: US 11/627.320 de 25/01/2007.

(54) Título: AGENTES DE PROTEÇÃO E MODOS DE PRIVILÉGIO.

(73) Titular: MICROSOFT TECHNOLOGY LICENSING, LLC. Endereço: One Microsoft Way, Redmond, Washington, ESTADOS UNIDOS DA AMÉRICA(US), 98052

(72) Inventor: ERIC TRAUT; FORREST FOLTZ; ANDREW J. THORNTON; SUYASH SINHA.

Prazo de Validade: 10 (dez) anos contados a partir de 13/11/2018, observadas as condições legais

Expedida em: 13/11/2018

Assinado digitalmente por:
Liane Elizabeth Caldeira Lage
Diretora de Patentes, Programas de Computador e Topografias de Circuitos Integrados

"AGENTES DE PROTEÇÃO E MODOS DE PRIVILÉGIO"

ANTECEDENTES

Os processadores dentro dos dispositivos de computação frequentemente incluem modos privilegiados e não privilegiados. O software funcionando em um modo privilegiado geralmente está apto a executar cada instrução suportada pelo processador. Tipicamente, o núcleo do sistema operacional funciona dentro do modo privilegiado, o qual algumas vezes é referido como "Anel 0", "Modo Supervisor", ou "Modo Núcleo".

Em contraste, algum software funcionando no dispositivo de computação pode ser restrito para funcionar somente em um modo não privilegiado. Este modo geralmente permite ao software funcionar um subgrupo de instruções do processador. Assim, um sistema operacional pode utilizar o modo não privilegiado para limitar a atividade do software funcionando neste modo. Por exemplo, o software pode ser restrito a um subconjunto particular de memória do dispositivo de computação. Este modo não privilegiado é algumas vezes conhecido como "Anel 3" ou "Modo do Usuário". Em geral, as aplicações do usuário do dispositivo de computação operam neste modo não privilegiado.

Se uma aplicação de software operar neste modo não privilegiado, a aplicação pode requisitar acesso a uma parte da memória que não pode ser diretamente acessada a partir do modo não privilegiado. Por exemplo, a aplicação pode desejar executar uma operação nesta parte da memória tal como "criar um novo arquivo". Esta requisição tipicamente é direcionada através de uma porta de chamada ou de outra instrução de chamada do sistema, a qual muda este código no modo não privilegiado para o código no modo privilegiado. Esta mudança garante que o modo não privilegiado não tenha acesso direto à memória que é designada como acessível a partir somente do modo privilegiado.

De acordo com estes modos, um autor de código malicioso pode acessar o modo privilegiado e instalar software mal intencionado que altera o comportamento do dispositivo de computação. Este software mal intencionado pode, por exemplo, alterar a localização de arquivos, ocultar arquivos, modificar arquivos, alterar digitações de tecla, e assim por diante. Alguns destes software mal intencionados podem compreender um "rootkit" (vírus), o qual não somente altera o comportamento do dispositivo de computação, mas também oculta ele próprio dentro da memória no modo privilegiado. As aplicações antivírus funcionando no dispositivo de computação por consequência podem falhar em descobrir este vírus oculto, assim permitindo ao software mal intencionado continuar suas ações mal intencionadas. Adicionalmente, tal software mal intencionado pode inserir código no sistema de proteção embutido no sistema operacional, como discutido abaixo.

O autor do software mal intencionado pode acessar o modo privilegiado e carregar o software mal intencionado em um dispositivo de computador de vários modos, incluindo enganar o usuário do dispositivo de computação para involuntariamente instalar o software

mal intencionado no próprio dispositivo de usuário. Como resultado, os sistemas operacionais atuais frequentemente empregam um ou mais sistemas de proteção para detectar tal software mal intencionado. Estes sistemas de proteção geralmente monitoram certos recursos importantes do sistema operacional para detectar quaisquer alterações junto a estes recursos. Se tal sistema de proteção detectar tal alteração, então, o sistema de proteção pode decidir que o recurso particular foi infectado pelo sistema mal intencionado. Estes sistemas de proteção também podem proporcionar, para a aplicação antivírus do usuário, uma lista de aplicações atualmente residentes na memória do modo não privilegiado. Obviamente, se o software mal intencionado teve sucesso em se ocultar, então ela não irá aparecer na lista proporcionada. Adicionalmente, se o software mal intencionado teve sucesso em inserir código no sistema de proteção, então, o sistema de proteção pode falhar ao funcionar ou de outro modo falhar em detectar quaisquer alterações junto aos recursos importantes do sistema operacional.

Enquanto estes sistemas de proteção podem ser eficazes, eles também podem sofrer de umas poucas fraquezas. Primeiro, estes sistemas frequentemente contam com o anonimato, e assim, estão vulneráveis á exploração se identificados pelo software mal intencionado. Ou seja, se o software mal intencionado decifra a identidade e localiza o sistema de proteção, ele pode desativar o próprio sistema de proteção. O autor do software mal intencionado também pode instruir outras pessoas sobre como fazer o mesmo. Adicionalmente e relacionado com o primeiro item, estes sistemas de proteção geralmente operam em um mesmo domínio de proteção que este do sistema operacional (por exemplo, dentro do próprio modo privilegiado). Portanto, o próprio sistema de proteção está sujeito a ataque se o software mal intencionado obter acesso ao modo privilegiado e estiver apto a desmascarar o sistema de proteção no anonimato. Finalmente, estes sistemas de proteção iniciam ao mesmo tempo que o sistema operacional ou que o modo privilegiado. Portanto, se o software mal intencionado ou o autor do software mal intencionado obter controle do dispositivo de computação antes desta inicialização, ele pode impedir o sistema de proteção de iniciar.

SUMARIO

Este documento descreve ferramentas capazes de tornar uma parte da memória do sistema operacional associada com uma agente de proteção inalterável ou inacessível a partir de um modo de privilégio do sistema operacional. Em algumas concretizações, estas ferramentas são capazes de criar uma modo de privilégio do agente de proteção por requisitar que um monitor virtual da máquina proteja esta parte da memória do sistema operacional. Em outras concretizações, estas ferramentas são capazes de criar o modo de privilégio do agente de proteção por virtualizar um processador físico dentro de vários processadores virtuais, pelo menos um dos quais é um processador virtual do agente de

proteção projetado para executar o agente de proteção. Por tornar esta parte da memória do sistema operacional inalterável ou inacessível a partir do modo de privilégio do sistema operacional, o agente de proteção pode ser menos vulnerável aos ataques por entidades operando dentro do modo de privilégio do sistema operacional.

Este Sumário é proporcionado para introduzir uma seleção de conceitos de uma forma simplificada que são adicionalmente descritos abaixo na Descrição Detalhada. Este Sumário não é pretendido para identificar aspectos chave ou essenciais do assunto reivindicado, nem é pretendido para ser utilizado como um auxílio ao determinar o escopo do assunto reivindicado. O termo "ferramentas", por exemplo, pode se referir ao sistema(s), método(s), instruções legíveis por computador, e/ou técnica(s) como permitidos pelo contexto acima e por todo o documento.

BREVE DESCRIÇÃO DOS DESENHOS

A Fig. 1 ilustra um ambiente operacional ilustrativo no qual várias concretizações das ferramentas podem operar.

A Fig. 2 demonstra a variação dos direitos de memória do dispositivo de computação dos módulos ilustrados na Fig. 1.

A Fig. 3 representa partes variadas da memória do dispositivo de computação nas quais alguns dos módulos ilustrados na Fig. 1 residem.

A Fig. 4 é um fluxograma ilustrando uma maneira ilustrativa na qual um monitor de máquina virtual pode proteger uma parte de memória associada com um agente de proteção e estabelecer um temporizador para executar o agente.

A Fig. 5 ilustra uma arquitetura ilustrativa possuindo um monitor de máquina virtual capaz de virtualizar processadores físicos em vários processador virtuais do sistema operacional e um processador virtual do agente de proteção.

A Fig. 6 ilustra como a largura de banda dos processadores físicos da Fig. 5 pode ser alocada dentre os vários processadores virtuais.

A Fig. 7 é um processo ilustrativo de alguns modos nos quais as ferramentas podem habilitar e executar um agente de proteção que reside em uma localização que é inacessível a partir de um modo de privilégio do sistema operacional.

A Fig. 9 é um processo ilustrativo de alguns modos nos quais as ferramentas podem criar um modo de privilégio do agente de proteção por fazer uma requisição para um monitor de máquina virtual.

A Fig. 10 é um processo ilustrativo de alguns modos nos quais as ferramentas podem criar um modo de privilégio do agente de proteção por virtualizar um processador real do computador em processadores virtuais do computador, pelo menos um dos quais é para executar um agente de proteção.

A Fig. 11 é um processo ilustrativo de alguns modos nos quais as ferramentas

podem permitir uma adição de um modo de privilégio não presente em um processador físico subjacente.

Os mesmos números são utilizados por toda a revelação e figuras para fazerem referência a componentes e aspectos iguais.

DESCRIÇÃO DETALHADA

Vista Geral

O documento a seguir descreve ferramentas capazes de operar um agente de proteção de uma maneira que torna o agente de proteção inalterável e inacessível a partir de um modo de privilégio do sistema operacional. Assim, estas ferramentas permitem a proteção do próprio agente de proteção, desse modo garantindo a habilidade do agente de proteção em detectar alterações junto a recursos importantes do sistema. Em adição, estas ferramentas podem encerrar um sistema operacional ou um modo de privilégio do sistema operacional em resposta a detectar alterações de recurso ou em resposta a uma tentativa de modificação do próprio agente de proteção. Adicionalmente, estas ferramentas podem permitir que o agente de proteção imponha invariância nos recursos do sistema operacional, sem a necessidade de detectar posteriormente a modificação do recurso.

Um ambiente no qual as ferramentas podem permitir estas e outras ações é exposto abaixo em uma seção denominada Ambiente Operacional Ilustrativo. Um seção denominada Agentes de Proteção Autônomos vem a seguir e inclui duas subseções. A primeira subseção, denominada Agentes de Proteção do Monitor de Máquina Virtual, descreve um modo ilustrativo no qual um agente de proteção pode residir e executar dentro de uma monitor de máquina virtual. Isto é seguido por outra subseção, denominada Agentes de Proteção de Partição Virtual, descrevendo um modo ilustrativo no qual um agente de proteção pode residir e executar dentro de uma partição virtual separada de uma partição do sistema operacional.

Outra seção denominada Modos de Privilégio do Agente de Proteção Autônomo vem a seguir e também inclui duas subseções. A primeira subseção descreve uma modo ilustrativo no qual um temporizador do monitor de máquina virtual pode adicionar um modo de privilégio do agente de proteção, e é denominada Requisições de Proteção para um Monitor de Máquina Virtual. Uma subseção denominada Processador Virtuais de Agente de Proteção vem a seguir e descreve outra maneira na qual um modo de privilégio do agente de proteção pode ser criado, neste caso, com o uso de vários processadores virtuais, incluindo um configurado para executar o agente de proteção no modo de privilégio do agente de proteção. Uma seção denominada Uso Ilustrativo das Ferramentas vem a seguir e descreve um exemplo das ferramentas anteriormente descritas em operação. Finalmente, uma seção denominada Outras Concretizações das Ferramentas descreve várias outras concretizações e maneiras nas quais as ferramentas podem atuar. Esta vista geral, incluindo

estes títulos de seção e resumos, é proporcionada para conveniência do leitor e não é pretendida para limitar o escopo das reivindicações ou das seções designadas.

Ambiente Operacional Ilustrativo

Antes de descrever as ferramentas em detalhes, a discussão seguinte de uma ambiente operacional ilustrativo é proporcionada para ajudar ao leitor a entender alguns modos nos quais vários aspectos da invenção das ferramentas podem ser empregados. O ambiente descrito abaixo constitui apenas um exemplo e não é pretendido para limitar a aplicação das ferramentas a qualquer ambiente operacional particular. Outros ambientes podem ser utilizados sem afastamento do espírito e do escopo do assunto reivindicado. Por exemplo, enquanto as seções seguintes descrevem concretizações com um único agente de proteção, vários agentes de proteção também podem ser utilizados. Em alguns casos, estes agentes de proteção podem funcionar independentemente e lado a lado. Em tais casos, os agentes de proteção tipicamente estão somente aptos a acessar memória dentro de sua respectiva partição. Adicionalmente, as técnicas descritas abaixo podem ser utilizadas simultaneamente. Ou seja, diferentes agentes de proteção podem utilizar diferentes técnicas dentro de um mesmo ambiente operacional.

Voltando-se para o exemplo corrente, a Figura 1 ilustra tal ambiente operacional geralmente designado por 100. Este ambiente inclui um dispositivo de computação 102, o qual ele próprio inclui um ou mais processadores 104 bem como meio legível por computador 106. O meio legível por computador 106 inclui um monitor de máquina virtual 108 (por exemplo, um virtualizador), o qual pode permitir a virtualização de um ou mais processadores em vários processadores virtuais. O monitor de máquina virtual 108 também pode permitir várias partições virtuais. Um ou mais processadores virtuais podem ser associados com cada partição, e estes processadores virtuais têm o trabalho regulado nos processadores físicos disponíveis. Como ilustrado, em algumas concretizações, o monitor de máquina virtual pode permitir uma primeira partição virtual 110 e uma segunda partição virtual 112. Como discutido em detalhes abaixo, estas partições podem servir para separar as funções do sistema operacional a partir dos serviços de agente de proteção.

Além disso, como ilustrado, o meio legível por computador 106 adicionalmente inclui um sistema operacional (OS) 114, bem como uma ou mais aplicações do usuário 116. O sistema operacional 114 proporciona serviços do sistema operacional 118 para as aplicações do usuário 116, assim permitindo que as aplicações funcionem no dispositivo de computação. Em adição, um ou mais recursos do sistema operacional 120 residem no sistema operacional. Recursos ilustrativos incluem uma tabela de expedição de serviço do sistema (SSDT), uma tabela de expedição de interrupção (IDT), uma tabela de descritor global (GDT) e assim por diante. Além disso, como ilustrado, o sistema operacional pode incluir software mal intencionado 122 (isto é, código com intenção maliciosa), o qual pode ter

sido carregado no dispositivo de computação de modos discutidos acima ou de outros modos. Um ou mais agentes de proteção, discutidos abaixo, podem detectar alterações feitas junto aos recursos do sistema operacional pelo software mal intencionado e, em resposta à detecção, executar ação defensiva. Se o agente fizer tal determinação, então o agente de proteção pode encerrar o sistema operacional e / ou o dispositivo de computação ou pode executar outra ação de contra-ataque.

Tendo discutido a estrutura do dispositivo de computação, a atenção agora é voltada para variar os modos de privilégio presentes nos um ou mais processadores físicos subjacentes 104. O modo de privilégio do monitor de máquina virtual 124 representa o modo mais privilegiado ilustrado na figura 1. Este modo de privilégio tem acesso a todos ou a substancialmente todos os recursos e memória do dispositivo. A partir do modo de privilégio do monitor de máquina virtual 124, o monitor de máquina virtual pode programas os processadores e permitir acesso às áreas de memória para cada partição virtual. Enquanto um sistema operacional funcionando dentro de uma partição pode acreditar que ele controla todos os recursos de um processador físico, na verdade ele somente controla uma parte como determinado pelo monitor de máquina virtual.

Menos privilegiado do que o modo de privilégio do monitor de máquina virtual, o modo de privilégio do sistema operacional 125 tem acesso a todos os recursos do sistema operacional 120 e à maior parte ou a toda a memória do sistema operacional. Este modo de privilégio, entretanto, não tem acesso a quaisquer recursos ou memória associados com outra partição, tal como a segunda partição virtual 112. Contudo, devido a este modo de privilégio geralmente ter acesso a toda a memória do sistema operacional, ele é algumas vezes referido como "Modo Privilegiado". "Anel 0", "Modo Supervisor", ou "Modo Núcleo" também podem descrever este modo de privilégio. Como discutido acima, uma aplicação do usuário operando dentro do modo de privilégio do sistema operacional 126 geralmente está apta a executar a maioria das instruções proporcionadas pelo processador, com a exceção desta instruções reservadas para o modo de monitor de máquina virtual.

Este modo de privilégio do sistema operacional está em contraste com o modo de privilégio do usuário 128, algumas vezes referido como "Modo Não Privilegiado", "Anel 3", ou simplesmente "Modo do Usuário". Além disso, como discutido acima, a aplicação do usuário pode não acessar ou alterar certa memória associada com o sistema operacional quando operando a partir do modo de privilégio do usuário 128. Em geral, as aplicações do usuário do dispositivo de computação operam neste modo de privilégio do usuário quando executando operações básicas.

Em adição aos modos discutidos acima, a figura 1 também ilustra um modo de privilégio de segunda partição virtual 130 e um modo de privilégio de agente de proteção 132. Como discutido em detalhes abaixo, o modo de privilégio de agente de proteção 132

pode ter acesso a uma parte da memória que o modo de privilégio do sistema operacional não possui, enquanto geralmente não tendo tanto acesso à memória quanto o modo de privilégio de monitor de máquina virtual. Como tal, este modo de privilégio pode ser mais privilegiado do que o modo de privilégio do sistema operacional mas menos privilegiado do que o modo de privilégio do monitor de máquina virtual.

Além disso, como discutido em detalhes abaixo, o modo de privilégio da segunda partição virtual geralmente tem acesso à memória associada com a segunda partição virtual 112. Em adição, este modo pode ter acesso à primeira partição virtual. Tal acesso adicional pode, por exemplo, permitir que um agente de proteção residindo na segunda partição virtual varra a memória associada com a primeira partição virtual e com seu correspondente sistema operacional. Este modo geralmente não tem acesso ao monitor de máquina virtual, e assim, é menos privilegiado do que o modo de privilégio de monitor de máquina virtual. Contudo, o modo de privilégio da segunda partição virtual ainda tem acesso a uma parte de memória que o modo de privilégio de sistema operacional não tem.

Enquanto isso, a figura 2 ilustra os direitos de memória do dispositivo de computação 200. Esta figura assim representa a quantidade de memória acessível pelos módulos da figura 1. Como ilustrado, o monitor de máquina virtual 108 – operando no modo de privilégio de monitor de máquina virtual 124 – possui a maior parte dos direitos de memória de todos módulos ilustrados. Na verdade, o monitor de máquina virtual reside, e sozinho tem acesso, a uma parte da memória 202. A seguir, o agente de proteção 204 (por exemplo, qualquer um dos agentes de proteção ilustrados na figura 1) opera no modo de privilégio de agente de proteção 132 e tem acesso a toda a memória diferente da parte 202 correspondendo ao monitor de máquina virtual. Entretanto, o agente de proteção realmente tem acesso a uma parte da memória 206, a qual é a parte da memória na qual o próprio agente de proteção reside.

O sistema operacional 114, enquanto isso, opera no modo de privilégio do sistema operacional 126 e tem acesso a toda a memória diferente da parte 202 e da parte 206. Enquanto o sistema operacional pode não acessar a parte da memória 206 associada com o agente de proteção, o sistema operacional e seu modo de privilégio associado realmente têm acesso a uma parte de memória 208. Esta parte de memória 208 é algumas vezes conhecida como memória núcleo ou componente de nível mais baixo de um sistema operacional e geralmente contém os recursos apresentados na figura 1. Mesmo se o software mal intencionado carregar e operar na parte de memória 208, entretanto, o software mal intencionado não pode acessar a parte de memória 206 associada com o agente de proteção.

Finalmente, a figura 2 ilustra que as aplicações do usuário 116 somente têm acesso a uma parte de memória 210. Estas aplicações do usuário e o modo de privilégio de usuário

correspondente não têm acesso à parte de memória 208 associada com o componente de nível mais baixo do sistema operacional. Com este ambiente operacional em mente, as quatro seções seguintes descrevem em detalhes modo ilustrativos nos quais um agente de proteção pode ser tornado inalterado ou inacessível a partir do modo de privilégio do sistema operacional.

Agentes de Proteção Autônomos

A seção seguinte descreve ferramentas capazes de determinar, a parir da memória inacessível por uma entidade operando dentro de um modo de privilégio do sistema operacional, se um ou mais recursos do sistema operacional foram modificados. Como tal, as ferramentas podem permitir que um agente de proteção resida em uma localização diferente da localização da própria memória do sistema operacional. Mais particularmente, as subseções seguintes descreve como os agentes de proteção podem residir dentro de um monitor de máquina virtual ou dentro de uma partição virtual autônoma.

Agentes de Proteção do Monitor de Máquina Virtual

Esta subseção descreve como um agente de proteção 134 pode residir dentro do próprio monitor de máquina virtual, como a figura 1 ilustra. Devido ao modo de privilégio de sistema operacional não poder acessar o monitor de máquina virtual, esta localização protege o agente de proteção de qualquer software mal intencionado localizado na memória de sistema operacional. De modo a operar a partir desta localização, o agente de proteção recebe uma identificação do um ou mais recursos do sistema operacional 120 que o agente de proteção 134 pode monitorar. Esta identificação pode ser recebida via o identificador de recurso 136. Como ilustrado, o sistema operacional pode proporcionar esta informação para o monitor de máquina virtual através de chamadas da interface de programação de aplicação (API), ou o sistema operacional pode proporcionar a informação na forma de um manifesto 138. Como discutido acima, estes recursos podem incluir a SSDT, IDT e a GDT.

Um vez que ele tenha recebido a identificação dos recursos, o agente de proteção 134 estende os serviços do agente de proteção 140 para o sistema operacional 114. Estes serviços do agente de proteção geralmente compreendem determinar se qualquer um dos recursos identificados foi alterado. Se tal determinação for feita, o agente de proteção ou o monitor de máquina virtual pode, por exemplo, encerrar o sistema operacional. Os serviços do agente de proteção também podem incluir impor invariância junto a quaisquer recursos marcados como inalteráveis (por exemplo, "somente leitura").

Empregar tal arquitetura começa com carregar e inicializar o monitor de máquina virtual, o qual é capaz de hospedar um ou mais sistemas operacionais. Neste exemplo, o monitor de máquina virtual hospeda um único sistema operacional 114, o qual ele próprio começa a inicialização após o monitor de máquina virtual carregar. Durante a inicialização do sistema operacional, a parte de memória 208 associada com o componente de nível mais

baixo do sistema operacional (por exemplo, o núcleo) carrega primeiro. Alguns ou todos os recursos do sistema operacional 120 (por exemplo, a SSDT, GDT, IDT) geralmente residem nesta parte de memória 208.

Antes ou enquanto o sistema operacional inicializa, o agente de proteção 134 pode começar a funcionar a partir de dentro do monitor de máquina virtual. Como discutido acima, o agente de proteção geralmente recebe uma identificação de um conjunto de um ou mais recursos do sistema operacional e determina se um ou mais dos recursos identificados foi alterado. Observe que cada recurso identificado frequentemente compreende vários componentes em várias localizações, cada um dos quais o agente de proteção pode monitorar de modo à totalmente proteger todo o recurso. Por exemplo, se o manifesto identifica uma SSDT como um recurso a ser monitorado e protegido, o agente de proteção não somente protege a tabela real mas também outros componentes da SSDT. Por exemplo, o agente de proteção também pode monitorar e varrer o registro que aponta para a localização da tabela. Adicionalmente, o agente de proteção também pode monitorar as estruturas de dados de tradução de memória (por exemplo tabelas de páginas) que traduzem o endereço virtual para um endereço físico. Se o agente de proteção falhar em fazer isto, então o código malicioso pode criar outra tabela com diferentes mapeamentos da tabela de páginas (isto é, desvia da própria SSDT).

Em adição à identificação, o agente de proteção também pode receber um atributo de proteção instruindo o agente de proteção sobre como proteger um recurso correspondente. Por exemplo, o agente de proteção pode receber uma identificação de um recurso SSDT, bem como um atributo de proteção correspondente de "somente leitura", e como tal, não deve ser alterado. "Inicia somente leitura" é outro atributo de proteção possível, o qual instrui o agente de proteção que o recurso correspondente pode gravar uma vez durante a inicialização, mas após tal tempo o recurso deve permanecer somente de leitura.

O agente de proteção pode receber esta identificação dos recursos e os atributos de proteção do recurso de vários modos, tanto positivamente como passivamente. Por exemplo, o sistema operacional pode proporcionar um manifesto assinado de forma digital que identifica os recursos que o agente de proteção pode monitorar. Este manifesto assinando de forma digital pode identificar os recursos de vários modos, tal como pelo nome (por exemplo, SSDT, IDT, GDT, etc.) ou pelo endereço, o qual mapeia o recurso para as localizações correspondentes na parte de memória 208. Nos últimos casos, o manifesto pode identificar um endereços físico convidado do recurso, um endereço virtual convidado, ou endereço físico do sistema. Observe que em alguns casos, um endereço físico convidado pode ser mapeado para um endereço físico real do sistema de modo a descobrir a localização física real do componente do recurso correspondente.

Após o monitor de máquina virtual ou agente de proteção receber o manifesto, estes componentes podem determinar se o manifesto foi adulterado ou modificado. De o monitor de máquina virtual ou o agente de proteção fizer tal determinação, o monitor de máquina virtual ou agente de proteção pode optar em falhar a inicialização do sistema operacional. Em adição, a criptografia associada com a lista de recursos pode ser invalidada, assim protegendo sua segurança.

Em adição ou em alternativa ao manifesto, o agente de proteção pode receber a identificação do recurso e o atributo de proteção via uma ou mais chamadas da interface de programação de aplicação (API) dentro do monitor de máquina virtual (por exemplo, "hypercalls"). À medida que o sistema operacional inicializa, o sistema operacional (e talvez o componente de nível mais baixo do sistema operacional 208) pode fazer hypercalls para dentro do monitor de máquina virtual informado ao agente de proteção sobre certos recursos que podem ser monitorados e protegidos. Estas hypercalls podem identificar os recursos pertinentes dos mesmos modos discutidos acima. Além disso, como discutido acima, estas hypercalls também podem identificar atributos de proteção do recurso.

Nas concretizações utilizando uma manifesto assinado de forma digital bem como uma ou mais hypercalls, o agente de proteção primeiro pode varrer os recursos identificados no manifesto antes ou enquanto o sistema operacional inicializa. Após esta varredura inicial, o sistema operacional então pode fazer hypercalls para o monitor de máquina virtual instruindo ao agente de proteção para determinar se páginas identificadas por hypercalls foram alteradas. O manifesto assim identifica recursos a serem varridos a cada inicialização do sistema operacional, enquanto as hypercalls identificam recursos a serem dinamicamente varridos quando de sua respectiva inicialização.

Tendo identificado os recursos a serem monitorados, o agente de proteção então determina se os recursos (por exemplo, todas as partes da SSDT discutidas acima) foram ou não alterados. O agente de proteção também pode impor invariância junto aos recursos identificados. Por exemplo, o agente de proteção pode garantir que qualquer recurso designado "somente leitura" não altere para "pode ser gravado".

De modo a monitorar e proteger os recursos deste modo, o código executando dentro do monitor de máquina virtual pode empregar um gerenciador de intercepção de monitor de máquina virtual (por exemplo, o gerenciador 146 da figura 1). Se assim instruído, este gerenciador de interceptação pode registrar interceptações nos vários componentes do recurso identificado. Devido a este registro, o agente de proteção dentro do monitor de máquina virtual pode agora receber interceptações se forem feitas tentativas de acessar ou modificar estes recursos identificados. Como tal, o agente de proteção pode inspecionar e varrer vários componentes dos recursos identificados. Ele também pode ativamente bloquear tentativas de modificar estes recursos.

Em algumas concretizações, o agente de proteção pode varrer os recursos e determinar um estado inicial dos recursos ao comparar os resultados de varreduras futuras. Em outras concretizações, o agente de proteção pode já conhecer um estado inicial dos recursos para comparar os resultados de varreduras futuras. Em qualquer caso, o agente de proteção pode calcular um valor hash (chave de codificação digital) ou de soma de verificação deste estado inicial. Após este cálculo, o agente de proteção varre os recursos antes, após, ou enquanto o sistema operacional inicializa. Após a varredura, o agente de proteção calcula um hash ou soma de verificação dos resultados e compara este com o valor hash ou soma de verificação do estado inicial. Se igual, o agente de proteção determina que os recursos correspondentes não foram alterados. Obviamente, o agente de proteção pode desviar os valores hash ou de soma de verificação e ao invés disso diretamente comparar o estado inicial com a varredura.

Se os valores forem diferentes, entretanto, o agente de proteção e/ou o monitor de máquina virtual pode executar uma ou mais ações de resposta. Primeiro, o próprio agente de proteção pode encerrar o sistema operacional ou o modo de privilégio de sistema operacional, ou ele pode instruir ao monitor de máquina virtual para fazer isto. Novamente, devido ao agente de proteção residir no monitor de máquina virtual e devido ao monitor de máquina virtual hospedar o sistema operacional, estes dois componentes são capazes de assim encerrar o sistema operacional. Adicionalmente, devido ao agente de proteção residir dentro do monitor de máquina virtual, o encerramento do sistema operacional não pode ser adulterado a partir de um igual modo de privilégio de sistema operacional.

Em adição a encerrar o sistema operacional, o agente de proteção e/ou o monitor de máquina virtual pode primeiro aviso ao sistema operacional sobre o encerramento eminente. Um canal de comunicação entre o monitor de máquina virtual e o sistema operacional pode permitir tal comunicação. Em alternativa, o agente de proteção e/ou o monitor de máquina virtual pode gravar um aviso em uma localização de memória ou sinalizar um evento que o sistema operacional monitora.

Sem considerar se um aviso foi ou não fornecido, o encerramento do sistema operacional pode ser abrupto ou harmonioso. No primeiro caso, o monitor de máquina virtual pode simplesmente desligar o sistema operacional imediatamente após o saber dos valores de hash ou de soma de verificação discrepantes. No último caso, o monitor de máquina virtual pode permitir ao sistema operacional uma certa quantidade de tempo para ele próprio se encerrar de forma limpa. Nesta hora, o sistema operacional pode, por exemplo, fechar quaisquer arquivos abertos e escoar quaisquer dados correspondentes. O sistema operacional também pode liberar recursos designados. Adicionalmente, o encerramento pode utilizar ambas as abordagens. Por exemplo, se o monitor de máquina virtual hospedar várias partições, ele pode imediatamente encerrar a partição com os valores de hash ou de

soma de verificação discrepantes enquanto permitindo às outras partições tempo para encerrar de forma clara. Em qualquer caso, a maneira do encerramento pode ser configurável pela política e pode ser ajustável.

Em adição a um encerramento e ao aviso correspondente, o agente de proteção e/ou monitor de máquina virtual pode executar ações após a inicialização em resposta a uma alteração não permitida de um recurso identificado. Por exemplo, o monitor de máquina virtual e / ou o agente de proteção pode, quando da reinicialização do sistema operacional, notificar ao sistema operacional sobre a alteração do recurso. Em resposta, o sistema operacional pode executar uma varredura antivírus para detectar se qualquer software mal intencionado efetivamente reside dentro da memória do sistema operacional, tal como a parte 208 (por exemplo, o núcleo). Adicionalmente, o monitor de máquina virtual pode inicializar o sistema operacional em um modo seguro, ou o próprio sistema operacional pode escolher inicializar no modo seguro. Além disso, em resposta à notificação, o sistema operacional pode identificar a si próprio como tendo sido atacado e como tal, pode não permitir a si próprio acessar qualquer rede junto a qual ele se acopla.

Agentes de Proteção de Partição Virtual

O invés de residir dentro do próprio monitor de máquina virtual, um agente de proteção (por exemplo, agente de proteção 142 da figura 1) pode residir em uma partição virtual separada (por exemplo, segunda partição virtual 112 da figura 1). Nestas concretizações, esta partição atua como um emissário confiável do monitor de máquina virtual. O agente de proteção 142 é assim inacessível a partir do modo de privilégio de sistema operacional. Como discutido acima, o monitor de máquina virtual 108 proporciona tal virtualização do dispositivo de computação 102. Enquanto o monitor de máquina virtual pode virtualizar o dispositivo de computação em qualquer número de partições, a figura 1 ilustra uma primeira partição hospedando o sistema operacional e uma segunda partição hospedando o agente de proteção. A segunda partição virtual na qual o agente de proteção reside pode ser, em alguns casos, uma partição de segurança dedicada cuja única função ou função principal é executar o agente de proteção. Em outras concretizações, esta segunda partição virtual pode executar funções adicionais, tal como hospedar outro sistema operacional.

O agente de proteção 142 residindo dentro da segunda partição virtual é capas de executar várias ou todas as mesmas funções que descritas acima com respeito ao agente de proteção 134 residindo dentro do monitor de máquina virtual. Ou seja, o agente de proteção 142 pode positivamente ou passivamente receber uma identificação de um ou mais recursos do sistema operacional 120. Em resposta à identificação, o agente de proteção pode novamente estender os serviços do agente de proteção 140, os quais geralmente compreendem determinar se um ou mais dos recursos identificados foi alterado e, se foi,

executar ação de resposta. Estes serviços também podem incluir impor invariância de recursos específicos. O agente de proteção 142 pode executar estas funções via técnicas similares a estas descritas acima.

Como ilustrado, o agente de proteção 142 é acessível a partir do modo de privilégio de segunda partição virtual 130, mas inacessível a partir do modo de privilégio de sistema operacional 126. Como tal, a arquitetura resultante permite a proteção do próprio agente de proteção de qualquer software mal intencionado localizado dentro do sistema operacional, mesmo se o software mal intencionado residir dentro da parte de memória 208 associada com o componente de nível mais baixo do sistema operacional.

Modos de Privilégio de Agente de Proteção Autônomo

Esta seção descreve ferramentas capazes de tornarem uma parte da memória do sistema operacional associada com um agente de proteção inalterável ou inacessível a partir de um modo de privilégio de sistema operacional, enquanto ainda permitindo a esta parte de memória fisicamente residir em um espaço de memória físico do sistema operacional. Estas ferramentas assim criam um modo de privilégio de agente de proteção autônomo que tem acesso à parte de memória associada com o agente de proteção bem como ao resto da memória que é acessível dentro do modo de privilégio de sistema operacional. Este modo de privilégio é assim mais privilegiado do que o modo de privilégio de sistema operacional.

A primeira subseção descreve ferramentas que são capazes de criar o modo de privilégio de agente de proteção por requisitar que um monitor de máquina virtual proteja uma parte de memória associada com o agente de proteção. Contudo, a segunda subseção descreve ferramentas que permitem a criação do modo de privilégio de agente de proteção pela virtualização de um processador físico em vários processadores virtuais, incluindo um processador virtual dedicado para executar o agente de proteção.

Requisições de Proteção para um Monitor de Máquina Virtual

Esta subseção descreve como um agente de proteção pode requisitar a um monitor de máquina virtual para proteger a memória associada com o agente de proteção e, como tal, o próprio agente de proteção. Esta proteção resulta em um agente de proteção 144 operando no modo de privilégio de agente de proteção 132, como ilustrado na figura 1. Como ilustrado, o agente de proteção 144 pode inicialmente residir dentro do modo de privilégio de sistema operacional, antes de mudar para o modo de privilégio de agente de proteção. Quando operando neste último modo de privilégio, o agente de proteção é geralmente impenetrável a ataques a partir de entidades operando no modo de privilégio de sistema operacional 126.

Quando operando no modo de privilégio de agente de proteção 132, um entidade possui ligeiramente mais privilégio do se operando no modo de privilégio de sistema

operacional 126, mas ainda menos privilégio do que o modo de privilégio de monitor de máquina virtual 124. Como a figura 2 ilustra, um agente de proteção operando neste modo de privilégio possui acesso a toda a memória associada com o sistema operacional, em adição à parte de memória 206 associada com o próprio agente de proteção. O monitor de máquina virtual 108 impõe a capacidade de acesso de agente de proteção adicionada.

As figuras 3 e 4 ilustram uma maneira ilustrativa de criar este modo de privilégio de agente de proteção. A figura 3 representa toda ou substancialmente toda a memória do dispositivo de computação 300. A memória do dispositivo de computação 300 inclui uma parte de memória 302 associada com o modo de privilégio de sistema operacional (por exemplo, o núcleo) e uma parte de memória 304 associada com o modo de privilégio de usuário. A parte de memória 302 também inclui, como ilustrado, uma parte de memória 306 associada com o agente de proteção 144 bem como uma parte de memória 308 na qual os controladores carregam.

Como a figura 4 ilustra, um processo 400 para criar o modo de privilégio de agente de proteção 132 começa no ato 1 pela inicialização da parte de memória 302 (por exemplo, núcleo). No ato 2, a parte de memória 306 ou o próprio agente de proteção chama o monitor de máquina virtual 108 para requisitar que o monitor de máquina virtual proteja a parte de memória associada com o agente de proteção. Ao requisitar, o agente de proteção ou a memória correspondente solicita que o código funcionando dentro do modo de privilégio de sistema operacional seja desabilitado para alterar ou de outro modo tocar esta parte de memória 306. O agente de proteção também pode ele mesmo verificar (por exemplo, por uma assinatura digital) junto ao monitor de máquina virtual 108. Esta parte de memória, ou o próprio agente de proteção, também pode requisitar que o monitor de máquina virtual estabeleça um temporizador e execute o agente de proteção quando o temporizador expirar. O ato 3 representa o monitor de máquina virtual protegendo a memória de entidades operando dentro do modo de privilégio de sistema operacional e estabelecendo um temporizador em resposta à requisição. Observe que devido a esta parte de memória 306 associada com o agente de proteção estar agora inalterável e/ou inacessível a partir do modo de privilégio de sistema operacional, o agente de proteção agora reside no modo de privilégio de agente de proteção.

No ato 4, os controladores são carregados na parte de memória 308. Observe que a requisição do ato 2 e a proteção correspondente do ato 3 geralmente ocorrem antes dos controladores serem carregados na memória, à medida que o software mal intencionado pode existir na forma de um controlador. Como discutido na seção "Uso Ilustrativo das Ferramentas" abaixo, os autores de software mal intencionado frequentemente enganam os usuários para instalarem controladores mal intencionados em um dispositivo de computação. Se um ou mais controladores mal intencionados realmente forem carregados

na memória antes da parte de memória 306 ser protegida, então os controladores mal intencionados podem potencialmente inserir código na requisição para se protegerem. Tal inserção de código desse modo impediria o funcionamento periódico do agente de proteção via o monitor de máquina virtual e, por conseqüência, a criação do modo de privilégio de agente de proteção. Entretanto, por requisitar que o monitor de máquina virtual estabeleça um temporizador inicialmente, este processo garante que código dentro do modo de privilégio de sistema operacional não possa de esse modo desabilitar o funcionamento periódico do agente de proteção.

Entretanto, o ato 5 provavelmente ocorre algum tempo após os controladores terem sido carregados. Como ilustrado, o ato 5 representa a expiração do temporizador do monitor de máquina virtual e, por conseqüência, o funcionamento do agente de proteção. Quando funcionando, o agente de proteção 144 executa funções similares ou idênticas a estas discutidas nas seções anteriores. Além disso, como discutido acima, o agente de proteção pode executar ação em resposta a uma determinação de que um ou mais recursos identificados foram alterados. O agente de proteção também pode executar tal ação em resposta a um acesso ou alteração tentada do agente de proteção, ou de sua memória correspondente, a partir de entidades operando dentro do modo de privilégio de sistema operacional.

O ato 6 representa o agente de proteção notificando para o monitor de máquina virtual quando o agente de proteção termina a execução. Finalmente, o ato 7 representa a repetição dos atos 3, 5 e 6. Como tal, o monitor de máquina virtual pode reiniciar seu temporizador e executar o agente de proteção em intervalos periódicos, tal como a cada 100 milisegundos (ms).

Por estabelecer um temporizador seguro contra falha no monitor de máquina virtual, o processo 400 desse modo elimina a habilidade do código do sistema operacional adulterar a parte de memória associada com o agente de proteção. Como tal, este processo garante que o agente de proteção irá continuar a funcionar e não terá código inserido por software mal intencionado atuando dentro do modo de privilégio de sistema operacional. Ao invés disso, o agente de proteção irá funcionar dentro de um modo de privilégio autônomo enquanto ainda residindo dentro da memória física alocada para o sistema operacional.

Processadores Virtuais de Agente de Proteção

Esta subseção descreve como um monitor de máquina virtual pode criar um modo de privilégio de agente de proteção por programar um processador virtual para executar o agente de proteção 144. A Figura 5 ilustra uma arquitetura 500 que inclui o monitor de máquina virtual 108 virtualizando o dispositivo de computação 102 em duas partições, cada uma incluindo um sistema operacional. Como ilustrado, o dispositivo de computação neste exemplo inclui dois processadores reais 104(a) e 104(b), em cada um dos quais o

processador virtual pode programar múltiplos processadores virtuais. Também como ilustrado, o monitor de máquina virtual cria uma primeira partição virtual 502 e uma segunda partição virtual 504. A primeira partição virtual inclui um primeiro processador virtual 506 para executar um primeiro sistema operacional. De forma similar, a segunda partição virtual inclui um segundo processador virtual 508 para executar um segundo sistema operacional. Neste caso, entretanto, o monitor de máquina virtual também inclui um processador virtual de agente de proteção 510 para executar um agente de proteção, tal como o agente de proteção 144 da figura 1.

Para criar a arquitetura 500, o monitor de máquina virtual primeiro é carregado e inicializado. Como ilustrado na figura 6, o monitor de máquina virtual então virtualiza os vários processadores virtuais e, ao fazer isso, aloca largura de banda de processador real 600. Para começar esta virtualização e alocação, o monitor de máquina virtual virtualiza o primeiro processador virtual sobre o primeiro processador real. No exemplo corrente, esta virtualização é feita em uma base de um para um como ilustrado pela figura 6. Ou seja, somente este único processador virtual 506 corresponde ao processador real 104(a) e, como tal, o monitor de máquina virtual aloca toda a largura de banda do processador real para este processador virtual. O monitor de máquina virtual então virtualiza o segundo processador virtual 508, sobre o segundo processador real 104(b). Ao invés de uma base de um para um, entretanto, o monitor de máquina virtual retém alguma parte da largura de banda do segundo processador real. O monitor de máquina virtual então virtualiza o processador virtual do agente de proteção 510 sobre esta largura de banda restante do segundo processador real 104(b), também como ilustrado pela figura 6.

Cada processador virtual operando no segundo processador real geralmente atua em uma base de tempo repartido. Ou seja, o segundo processador virtual pode operar no segundo processador real durante algum tempo, antes da operação do segundo processador virtual suspender. Neste ponto, o segundo processador real troca para a operação do processador virtual do agente de proteção durante alguma outra quantidade de tempo. Por exemplo, o segundo processador virtual pode operar no segundo processador real durante 90 ms, ponto no qual a operação deste segundo processador virtual é suspensa e a operação do processador virtual de agente de proteção começa durante 10 ms. O processador virtual de agente de proteção geralmente é transparente para ambas as partições do sistema operacional e para ambos os primeiro e segundo processadores virtuais. Como tal, ambos os sistemas operacionais acreditam que seus processadores virtuais correspondentes correspondem a um respectivo processador real.

Em adição a alocar a largura de banda do processador real, o monitor de máquina virtual também gerencia a parte de memória que cada processador virtual pode acessar. No exemplo corrente, o primeiro processador virtual pode acessar toda a memória associada

com o primeiro sistema operacional. O segundo processador virtual, entretanto, pode acessar toda a memória associada com o segundo sistema operacional, diferente da parte de memória associada com o agente de proteção. O processador virtual de agente de proteção sozinho tem acesso á parte de memória associada com o agente de proteção, em adição à memória alocada para o segundo sistema operacional.

Adicionalmente, o primeiro e o segundo processadores virtuais somente têm a habilidade de alterar sua memória associada. Como tal, nenhum dos processadores virtuais operando seus respectivos sistemas operacionais pode alterar a parte de memória associada com o agente de proteção. O processador virtual do agente de proteção, entretanto, pode alterar a memória associada com o agente de proteção e, em algumas concretizações, a memória associada com o segundo processador virtual.

Por sua natureza programada, o processador virtual de agente de proteção irá periodicamente executar o agente de proteção. Enquanto em alguns casos o processador virtual de agente de proteção pode executar outras aplicações, o exemplo corrente ilustra um processador virtual de agente de proteção dedicado. Como tal, este processador virtual geralmente somente serve para periodicamente executar o agente de proteção. Novamente, o agente de proteção pode executar funções similares ou idênticas, de maneiras similares ou idênticas, da mesma forma que os agentes de proteção descritos acima.

Por programar um processador virtual de agente de proteção dedicado, o monitor de máquina virtual garante que o agente de proteção irá periodicamente executar sob controle deste processador e de um modo de privilégio de agente de proteção autônomo. Adicionalmente, devido a somente este processador virtual de agente de proteção ter acesso à parte de memória associada com o agente de proteção, o monitor de máquina virtual protege esta memória de código dentro de um sistema operacional. Portanto, software mal intencionado dentro de um modo de privilégio de sistema operacional não pode inserir código no agente de proteção e impedir o agente de proteção de funcionar. Como tal, esta técnica essencialmente elimina a habilidade de um sistema operacional de adulterar o agente de proteção.

Uso Ilustrativo das Ferramentas

Tendo anteriormente descrito ferramentas capazes de garantir proteção de um agente de proteção, a seção seguinte descreve apenas um exemplo destas ferramentas em operação. Primeiro, imagine que um usuário do computador surfa na Internet e, enquanto surfando por certo Site da internet, uma caixa de diálogo com intenção maliciosa surge de repente no vídeo do usuário. A caixa de diálogo requisita permissão a partir do usuário para instalar algum tipo de software mal intencionado no computador de um usuário. Apesar de esta requisição poder ser direta, imagine que a caixa de diálogo oculta a requisição como tipicamente é o caso. A caixa de diálogo pode, por exemplo, falsamente informar para o

usuário que ele ou ela ganhou um prêmio. Ao informar isso, a caixa de diálogo maliciosamente instrui ao usuário para clicar o botão "OK" na caixa de diálogo de modo a receber o prêmio. Imagine que o usuário realmente selecione o botão OK e assim o usuário escolhe continuar as operações requisitadas independente de um ou mais avisos a partir do software (por exemplo, uma aplicação antivírus) funcionando no dispositivo de computação.

Neste ponto, o dispositivo de computação começa a instalação de um controlador que contém o software mal intencionado. Como é geralmente verdadeiro com os controladores, este controlador malicioso tem acesso concedido para um modo de privilégio de sistema operacional e é carregado na memória associada com este modo de privilégio (por exemplo, o núcleo). Uma vez carregado no núcleo, o controlador malicioso e seu software mal intencionado acompanhante essencialmente possuem acesso com carta branca à memória do computador e ao sistema operacional. Infelizmente para o usuário, imagine que este software mal intencionado inclui um registrador cronológico de tecla que registra as digitações de tecla de um usuário. Agora imagine que o usuário navega para o site da Internet do seu banco e entra em sua conta bancária. Devido a sua habilidade de registrar as digitações de tecla, o registrador cronológico de tecla aprende a senha da conta bancária do usuário e envia esta senha através da Internet para o autor do controlador malicioso.

Para tornar a situação pior, imagine que o software mal intencionado é um "rootkit" – ou software mal intencionado que tenta ativamente se ocultar de um agente de proteção e do software antivírus do usuário. Nos sistemas convencionais, um agente de proteção reside dentro do núcleo (isto é, na memória junto a qual o controlador malicioso tem acesso). Portanto, nestes sistemas convencionais, o software mal intencionado tem acesso ao agente de proteção e pode tentar se ocultar do agente de proteção. Se obtiver sucesso, o software mal intencionado iria aparecer para o agente de proteção como não existindo dentro do núcleo. Portanto, quando o software antivírus do usuário chama o agente de proteção e requisita uma lista de todas as aplicações presentes na memória do computador, o software mal intencionado estaria ausente. Esta ausência torna o software antivírus ineficaz para saber e remover o software mal intencionado. Adicionalmente, o software mal intencionado pode inserir código no agente de proteção, desse modo impedindo o agente de proteção de funcionar. Como tal, o agente de proteção pode falhar em perceber se o software mal intencionado alterar quaisquer recursos do sistema operacional.

Ao invés de residir dentro do núcleo como nos sistemas convencionais, entretanto, imagine que o agente de proteção no dispositivo de computação do usuário reside na memória ou funciona em um modo que é inacessível a partir do modo de privilégio de sistema operacional. Portanto, quando o controlador malicioso é carregado no núcleo, ele não tem acesso á memória na qual o agente de proteção reside ou ao modo no qual o

agente de proteção funciona. Por conseqüência, o controlador e seu software mal intencionado acompanhante não possuem acesso ao próprio agente de proteção. O software mal intencionado então está inapto a se ocultar do agente de proteção e por conseqüência, também do software antivírus. Portanto, quando o software antivírus solicita ao agente de proteção uma lista de todas as aplicações presentes na memória do computador, a lista retornada inclui o software mal intencionado. O software antivírus então reconhece este código como software mal intencionado e por consequência remove o mesmo do dispositivo de computador do usuário. Adicionalmente, o próprio agente de proteção pode perceber se o software mal intencionado altera recursos do sistema operacional e em resposta, pode encerrar o dispositivo de computação do usuário.

Portanto, por residir na memória ou funcionar em um modo que é inacessível a partir do modo de privilégio de sistema operacional, as concretizações descritas neste documento impedem software mal intencionado de se ocultar de um agente de proteção ou de inserir código no agente de proteção. No exemplo acima, portanto, o dispositivo de computação do usuário está apto a remover o software mal intencionado da máquina ou, em alguns casos, encerrar o sistema quando o software mal intencionado altera recursos importantes. Em qualquer caso, estas concretizações servem para diminuir a eficácia do software mal intencionado em relação ao seu desejo de causar dano.

Outras Concretizações das Ferramentas

As seções acima descrevem alguns exemplos particulares onde um agente de proteção é feito inalterado ou inacessível a partir do modo de privilégio de sistema operacional. Nesta seção, outras concretizações das ferramentas são descritas, tal como adicionar um modo de privilégio para um processador que não está presente em um processador subjacente.

Estas concretizações ilustrativas são descritas como partes do processo 700 até 1100 das figuras 7 até 11. Estes processos, bem como os processos ilustrativos descritos ou ilustrados com referência às figuras 1 até 6, podem ser implementados em qualquer hardware, software, firmware, ou em combinações dos mesmos; no caso de software e firmware, estes processos representam grupos de operações implementadas como instruções legíveis por computador armazenadas em meio legível por computador e executáveis por um ou mais processadores. Estas concretizações das ferramentas descritas nesta seção não são pretendidas para limitar o escopo das ferramentas ou das reivindicações.

Com referência à figura 7, o bloco 702 recebe uma política de imposição identificando um ou mais recursos do sistema operacional. Esta política de imposição, a qual pode compreender dados criptografados, pode ser recebida via um manifesto assinado de forma digital ou pela exposição de um interface de programa de aplicação (API) ao sistema

operacional (por exemplo, hypercall). O bloco 704 identifica, a partir da memória inacessível a partir de uma entidade operando dentro de um modo de privilégio de sistema operacional, um ou mais recursos do sistema operacional. Recursos ilustrativos incluem uma tabela de expedição de serviços do sistema (SSDT), uma tabela de expedição de interrupção (IDT), e / ou uma tabela de descritor global (GDT). Como descrito acima, esta identificação pode ocorrer dentro de um monitor de máquina virtual (por exemplo, pelo agente de proteção 134 da figura 1) ou dentro de uma partição virtual separada (por exemplo, pelo agente de proteção 142 da figura 1).

Enquanto isso, o bloco 706 representa determinar se qualquer um dos recursos identificados foi alterado. Novamente, isto pode acontecer dentro de um monitor de máquina virtual ou dentro de uma partição separada. Se o bloco 706 determinar que um ou mais dos recursos identificados realmente foi alterado, então o bloco 708 termina o sistema operacional em resposta a esta determinação. Finalmente, o bloco 710 notifica ao sistema operacional sobre uma operação ilegal quando da reinicialização do sistema operacional.

A figura 8 ilustra um processo 800 para permitir a um agente de proteção funcionar dentro de um monitor de máquina virtual. O bloco 802 altera um gerenciador de interceptação de monitor de máquina virtual eficaz para permitir a recepção de uma identificação de que uma página da memória ou registrador associado com uma recurso do sistema operacional foi alterado. Este recurso pode compreender um dos recursos descritos com referência à figura 7, ou pode ser outro recurso do sistema operacional. Em qualquer caso, o bloco 804 recebe uma política de imposição identificando o recurso do sistema operacional e possivelmente um ou mais outros recursos do sistema operacional. Novamente, esta identificação pode ser feita via as técnicas discutidas acima. Como descrito acima, um atributo de proteção (por exemplo, "somente leitura" ou "inicialização somente leitura") do recurso pode acompanhar a identificação do recurso. O bloco 806, enquanto isso, representa a recepção de uma indicação de que a página ou registrador da memória associado com o recurso do sistema operacional realmente foi alterada. Em resposta, o bloco 808 encerra um modo de privilégio de sistema operacional eficaz em encerrar um sistema operacional associado com o recurso do sistema operacional. Em alguns casos, o monitor de máquina virtual 108 da figura 1 pode realizar este encerramento do modo de privilégio de sistema operacional.

A seguir, a figura 9 descreve um processo ilustrativo 900 para criar um modo de privilégio de agente de proteção, tal como o modo de privilégio de agente de proteção 132 ilustrado na figura 1. O bloco 902 recebe uma requisição de que uma faixa particular de memória seja feita inalterável ou inacessível a partir de um modo de privilégio de sistema operacional. Novamente, um monitor de máquina virtual pode receber esta requisição, a qual pode se originar a partir da própria faixa de memória ou a partir de um agente de

proteção residindo na faixa de memória. O bloco 904 protege a faixa de memória e estabelece um temporizador para periodicamente executar o agente de proteção residindo na faixa de memória. Novamente, um monitor de máquina virtual pode estabelecer tal temporizador, o qual pode instruir o monitor de máquina virtual para executar o agente de proteção em intervalos regulares.

Enquanto isso, o bloco 906 recebe uma política de imposição descrevendo um recurso do sistema operacional. Novamente, a política de imposição e o recurso descrito podem ser similares ou idênticos a estes discutidos acima. O bloco 908 executa o agente de proteção, o qual pode ser obtido pelo monitor de máquina virtual. O bloco de decisão 910 questiona se o recurso do sistema operacional foi alterado. O agente de proteção pode fazer esta determinar por funcionar da forma descrita em detalhes acima. Se o bloco 910 realmente determinar que uma alteração ocorreu, então o bloco 812 encerra o sistema operacional. Entretanto, se nenhuma determinação for feita, então o bloco 914 recebe uma notificação de que o agente de proteção terminou a execução. Em alguns casos e como descrito acima, o próprio agente de proteção pode desse modo notificar o monitor de máquina virtual. O bloco 916, enquanto isso, representa a ciclagem entre executar o agente de proteção e não executar o agente de proteção. Finalmente, observe que enquanto o agente de proteção não executa, o monitor de máquina virtual pode encerrar o sistema operacional em resposta a um acesso tentado a partir de uma entidade operando dentro do modo de privilégio de sistema operacional, da faixa de memória associada com o agente de proteção.

A figura 10 ilustra outro processo ilustrativo 1000 para criar um modo de privilégio de agente de proteção, tal como o modo de privilégio de agente de proteção 132 ilustrado na figura 1. O bloco 1002 virtualiza um processador de computador real em vários processadores de computador virtuais. Estes processadores virtuais podem compreender um ou mais processadores virtuais de sistema operacional, cada um possuindo um privilégio para alterar sua própria memória do sistema operacional e utilizar uma parte de uma largura de banda de processamento dos processadores reais, como ilustrado na figura 6. Os processadores virtuais também podem incluir pelo menos um processador virtual de agente de proteção possuindo um privilégio para alterar sua própria memória de agente de proteção e utilizar uma parte diferente da largura de banda de processamento dos processadores reais. Enquanto todos os processadores virtuais podem ser programados pelo monitor de máquina virtual, o processador virtual de agente de proteção pode ser transparente para os processadores virtuais de sistema operacional. Em alguns casos, os processadores virtuais de sistema operacional podem ser incapazes de alterar memória designada para o processador virtual de agente de proteção. Adicionalmente, o processador virtual de agente de proteção pode ser um processador dedicado cujo propósito principal ou único é causar

que o agente de proteção execute, como discutido acima.

A seguir, o bloco 1004 causa que o processador virtual de agente de proteção execute um agente de proteção, o qual pode ser eficaz para determinar se uma parte da dita memória do sistema operacional foi ou não alterada. O bloco 1006, enquanto isso, recebe uma indicação de que uma parte da memória de sistema operacional foi alterada. Em resposta, o bloco 1008 encerra um sistema operacional correspondente.

Finalmente, a figura 11 representa um processo 1100 para adicionar um modo de privilégio para um processador de computação real. O bloco 1102 representa a determinação, identificação, ou classificação de um ou mais modos de privilégio presentes em um processador físico subjacente. Estes modos de privilégio são geralmente definidos pelo próprio processador físico subjacente. De qualquer forma, o bloco 1104 adiciona um modo de privilégio que não está presente no processador físico subjacente. Em alguns casos, o modo de privilégio adicionado é capaz de alterar uma parte de memória do dispositivo de computação que é diferente de uma parte de memória que pode ser alterada por um ou mais modos de privilégio presentes. O modo de privilégio adicionado também pode ser capaz de adicionar e executar instruções que anteriormente não existiam ou não eram executáveis no processador subjacente.

Adicionalmente, o um ou mais modos de privilégio presentes no processador físico subjacente podem incluir um modo de privilégio de usuário e um modo de privilégio de sistema operacional. Nestas concretizações, o modo de privilégio adicionado pode ser mais privilegiado do que tanto o modo de privilégio de usuário como o modo de privilégio de sistema operacional, mais privilegiado do que o modo de privilégio de usuário, mas menos privilegiado do que o modo de privilégio de sistema operacional, ou menos privilegiado do que ambos modos de privilégio do usuário e de sistema operacional. Finalmente, observe que um caso da adição do modo de privilégio pode compreender adicionar um modo de privilégio de agente de proteção (por exemplo, o modo de privilégio de agente de proteção 132 ilustrado na figura 1) dos vários modos discutidos acima. Por exemplo, um agente de proteção ou sua faixa de memória associada pode requisitar que a faixa de memória seja feita inacessível a partir de entidades operando dentro do modo de privilégio de sistema operacional. Um monitor de máquina virtual também pode criar este modo de privilégio por programar um processador virtual de agente de proteção para executar o agente de proteção.

Conclusão

As ferramentas descritas acima são capazes de tornar um agente de proteção inalterável ou inacessível a partir de um modo de privilégio de sistema operacional, por permitir que o agente de proteção resida em uma localização que é inacessível a partir do modo de privilégio de sistema operacional, ou por criar um modo de privilégio de agente de

proteção. Apesar das ferramentas terem sido descritas em linguagem específica para aspectos estruturais e/ou atos metodológicos, é para ser entendido que as ferramentas definidas nas reivindicações anexas não estão necessariamente limitadas aos aspetos ou aos atos específicos descritos. Ao invés disso, os aspectos e atos específicos são revelados como formas ilustrativas de implementação das ferramentas.

REIVINDICAÇÕES

1. Meio legível por computador, **CARACTERIZADO** por possuir instruções legíveis por computador no mesmo que, quando executadas por um dispositivo de computação (102), fazem com que o dispositivo de computação (102) execute atos, compreendendo:

receber (902), em um monitor de máquina virtual (108), uma requisição para que uma faixa de memória (205, 306) seja feita inalterável ou inacessível a partir de um modo de privilégio de sistema operacional (126);

tornar (904) a faixa de memória (206, 306) inalterável ou inacessível a partir do modo de privilégio de sistema operacional (126); e

executar (908) um agente de proteção (144) que reside dentro da faixa de memória (206,306).

2. Meio, de acordo com a reivindicação 1, **CARACTERIZADO** por adicionalmente compreender estabelecer (904) um temporizador para executar o agente de proteção (144).

3. Meio, de acordo com a reivindicação 2, **CARACTERIZADO** pelo fato de que o temporizador instrui o monitor de máquina virtual (108) para executar o agente de proteção (144) em intervalos regulares.

4. Meio, de acordo com a reivindicação 1, **CARACTERIZADO** pelo fato de que o agente de proteção (144) é configurado para receber (906) uma política de imposição descrevendo um ou mis recursos (120) acessíveis a partir do modo de privilégio de sistema operacional (126) e, em resposta à receber a política de imposição, determinar (910) se o um ou mais dentre o um ou mais recursos (120) oram alterados.

5. Meio, de acordo com a reivindicação 4, **CARACTERIZADO** por adicionalmente compreender encerra (912) um sistema operacional (114) associado com o modo de privilégio de sistema operacional (126) em resposta a uma determinação pelo agente de proteção (144) de que um ou mais dos um ou mais recursos (120) foram alterados.

6. Meio, de acordo com a reivindicação 4, **CARACTERIZADO** pelo fato de que o um ou mais recursos (120) incluem uma tabela de expedição de serviços do sistema (SSDT), uma tabela de expedição de interrupção (IDT), ou uma tabela de descritores globais (GDT).

7. Meio, de acordo com a reivindicação 1, **CARACTERIZADO** por adicionalmente compreender receber (914), no monitor de máquina virtual (108) e após a execução (908) do agente de proteção (144), uma notificação de que o agente de proteção (144) acabou de executar.

8. Meio, de acordo com a reivindicação 1, **CARACTERIZADO** por adicionalmente compreender encerrar um sistema operacional (114) associado com o modo de privilégio de sistema operacional (126) em resposta a uma tentativa de acesso a partir do modo de privilégio de sistema operacional (126), da faixa de memória (206, 306) ou do agente de

proteção (144).

9. Meio, de acordo com a reivindicação 1, **CARACTERIZADO** por adicionalmente compreender fazer um ciclo (916) entre a execução (908) do agente de proteção (144) e a não execução do agente de proteção (144), de modo que pelo menos quando o agente de proteção (144) executa, ele fica inalterável ou inacessível a partir do modo de privilégio de sistema operacional (126).

10. Método, **CARACTERIZADO** por compreender:

virtualizar (1002) um ou mais processadores de computação real (104(a), 104(b)) em processadores de computação virtual (506, 508, 510), os processadores de computação virtual (506, 508, 510) compreendendo:

um ou mais processadores virtuais de sistema operacional (506, 508), cada um possuindo um privilégio para alterar sua própria memória de sistema operacional e utilizar uma parte de uma largura de banda de processamento (600) do um ou mais processadores de computação reais (104(a), 104(c)); e

pelo menos um processador virtual de agente de proteção (510) possuindo um privilégio para alterar sua própria memória de agente de proteção e utilizar uma parte diferente da largura de banda de processamento (600) do um ou mais processadores de computação reais (104(a), 104(b)); e

fazer (1004) com que o processador virtual de agente de proteção (510) execute uma agente de proteção (144) eficaz para determinar se uma parte da dita memória de sistema operacional foi ou não alterada.

11. Método, de acordo com a reivindicação 10, **CARACTERIZADO** por adicionalmente compreender:

receber (1006) uma indicação de que o agente de proteção (144) determinou que a parte da dita memória de sistema operacional foi alterada; e

em resposta a recepção da indicação, encerrar (1008) um sistema operacional correspondente (114).

12. Método, de acordo com a reivindicação 10, **CARACTERIZADO** pelo fato de que o um ou mais processadores virtuais de sistema operacional (506, 508) são incapazes de alterar a memória de agente de proteção.

13. Método, de acordo com a reivindicação 10, **CARACTERIZADO** pelo fato de que o ato de causar (1004) que o processador virtual de agente de proteção (510) execute o agente de proteção (144) compreende causar que o processador virtual de agente de proteção (510) execute o agente de proteção (144) em intervalos de tempo especificados.

14. Método, de acordo com a reivindicação 10, **CARACTERIZADO** pelo fato de que o processador virtual de agente de proteção (510) é dedicado somente para executar o agente de proteção (144).

15. Método, de acordo com a reivindicação 10, **CARACTERIZADO** pelo fato de que o processador virtual de agente de proteção (510) é programado por um monitor de máquina virtual (108) e é transparente para um sistema operacional (114) associado com a dita memória de sistema operacional.

16. Meio legível por computador, **CARACTERIZADO** por possuir instruções legíveis por computador nos mesmos que, quando executadas por um dispositivo de computação (102) compreendendo um processador físico subjacente (104) que inclui um ou mais modos de privilégio, fazem com que o dispositivo de computação (102) adicione (1104) um modo de privilégio que não está presente no processador físico subjacente (104).

17. Meio, de acordo com a reivindicação 16, **CARACTERIZADO** pelo fato de que o modo de privilégio adicionado é capaz de alterar uma parte de memória do dispositivo de computação (102) que é diferente de uma parte de memória que é inalterável pelo um ou mais modos de privilégio que estão inicialmente presentes no processador físico subjacente (104).

18. Meio, de acordo com a reivindicação 16, **CARACTERIZADO** pelo fato de que o um ou mais modos de privilégio inicialmente presentes no processador físico subjacente (102) incluem um modo de privilégio de usuário (128) e um modo de privilégio de sistema operacional (126), e onde o modo de privilégio adicionado é mais privilegiado do que tanto o modo de privilégio de usuário (128) como o modo de privilégio de sistema operacional (126).

19. Meio, de acordo com a reivindicação 16, **CARACTERIZADO** pelo fato de que o um ou mais modos de privilégio inicialmente presentes no processador físico subjacente (104) incluem um modo de privilégio de usuário (128) e um modo de privilégio de sistema operacional (126), e onde o modo de privilégio adicionado é mais privilegiado do que o modo de privilégio de usuário (128), mas menos privilegiado do que o modo de privilégio de sistema operacional (126).

20. Meio, de acordo com a reivindicação 16, **CARACTERIZADO** pelo fato de que o um ou mais modos de privilégio inicialmente presentes no processador físico subjacente incluem um modo de privilégio de sistema operacional (126), e onde a adição (1104) do modo de privilégio compreende chamar um monitor de máquina virtual (108) para requisitar que uma faixa de memória (206, 306) associada com um agente de proteção (144) seja feita inalterável ou inacessível a partir do modo de privilégio de sistema operacional (126).

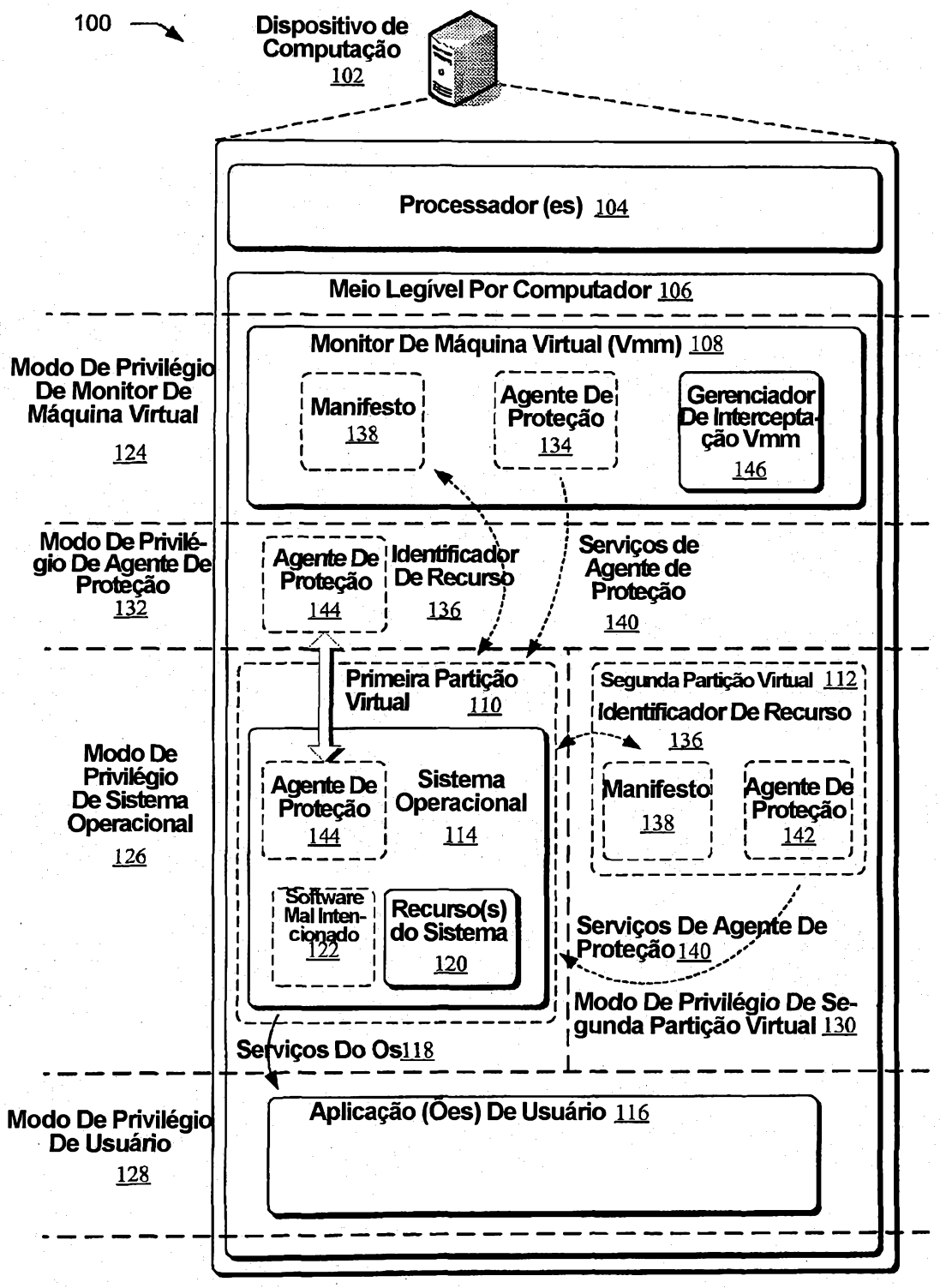
100
Dispositivo de Computação 102
Processador (es) 104
Meio Legível Por Computador 106
Monitor De Máquina Virtual (Vmm) 108
Manifesto 138
Agente De Proteção 134
Gerenciador De Interceptação Vmm 146
Modo De Privilégio De Monitor De Máquina Virtual 124
Modo De Privilégio De Agente De Proteção 132
Agente De Proteção 144
Identificador De Recurso 136
Serviços de Agente de Proteção 140
Primeira Partição Virtual 110
Segunda Partição Virtual 112
Identificador De Recurso 136
Modo De Privilégio De Sistema Operacional 126
Agente De Proteção 144
Sistema Operacional 114
Manifesto 138
Agente De Proteção 142
Software Mal Intencionado 122
Recurso(s) do Sistema 120
Serviços De Agente De Proteção 140
Modo De Privilégio De Segunda Partição Virtual 130
Serviços Do Os 118
Modo De Privilégio De Usuário 128
Aplicação (Ões) De Usuário 116

FIG. 1

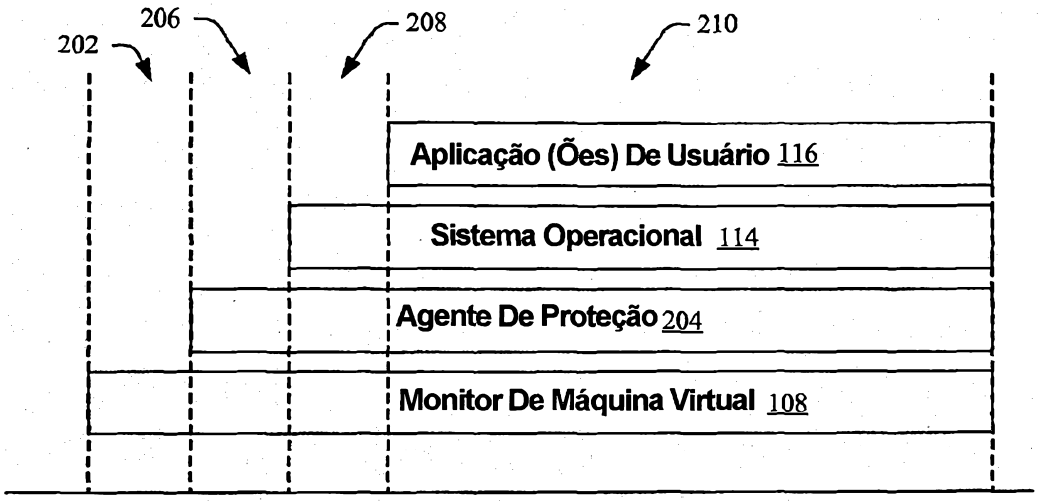
206
208
210
202
Aplicação (Ões) De Usuário 116
Sistema Operacional 114
Agente De Proteção 204
Monitor De Máquina Virtual 108
Direitos De Memória Do Dispositivo De Computação
200

FIG. 2

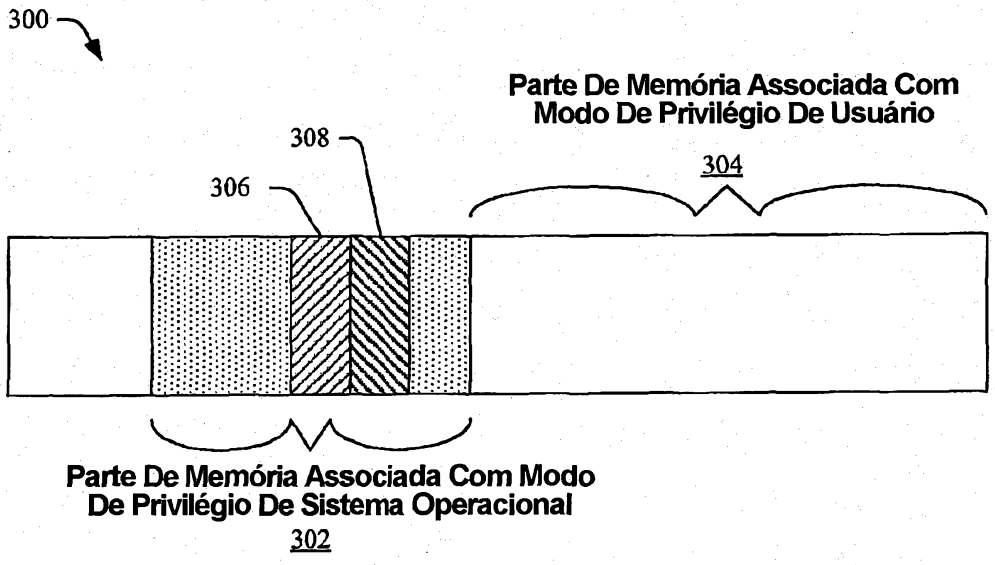
300
Parte De Memória Associada Com Modo De Privilégio De Usuário
308
306
304
Parte De Memória Associada Com Modo De Privilégio De Sistema Operacional
302

FIG. 3

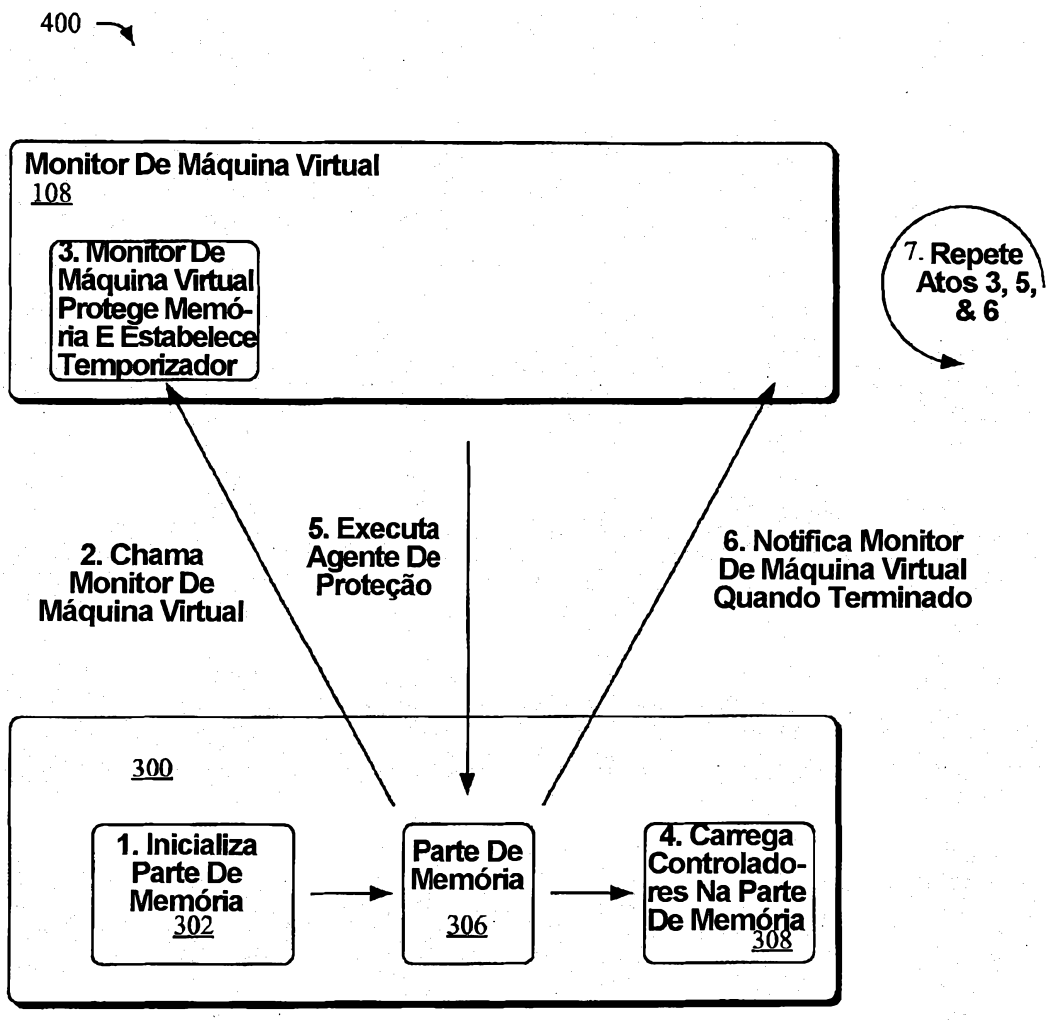
400
Monitor De Máquina Virtual
108
3. Monitor De Máquina Virtual Protege Memória E Estabelece Temporizador
7. Repete Atos 3, 5, & 6
2. Chama Monitor De Máquina Virtual
5. Executa Agente De Proteção
6. Notifica Monitor De Máquina Virtual Quando Terminado
300
1. Inicializa Parte De Memória
302
Parte De Memória
306
4. Carrega Controladores Na Parte De Memória
308

FIG. 4

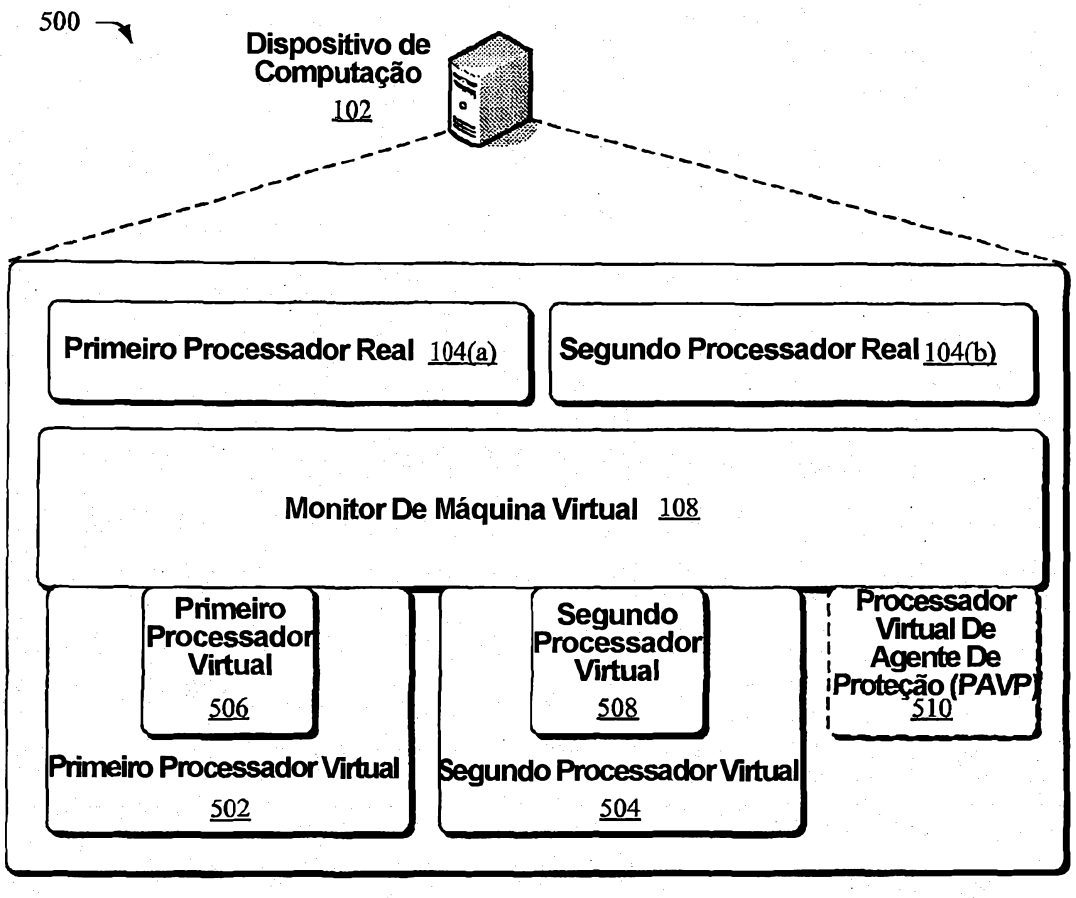
500
Dispositivo de Computação
102
Primeiro Processador Real 104(a)
Segundo Processador Real 104(b)
Monitor De Máquina Virtual 108
Primeiro Processador Virtual
506
Primeiro Processador Virtual
502
Segundo Processador Virtual
508
Segundo Processador Virtual
504
Processador Virtual De Agente De Proteção (PAVP)
510

FIG. 5

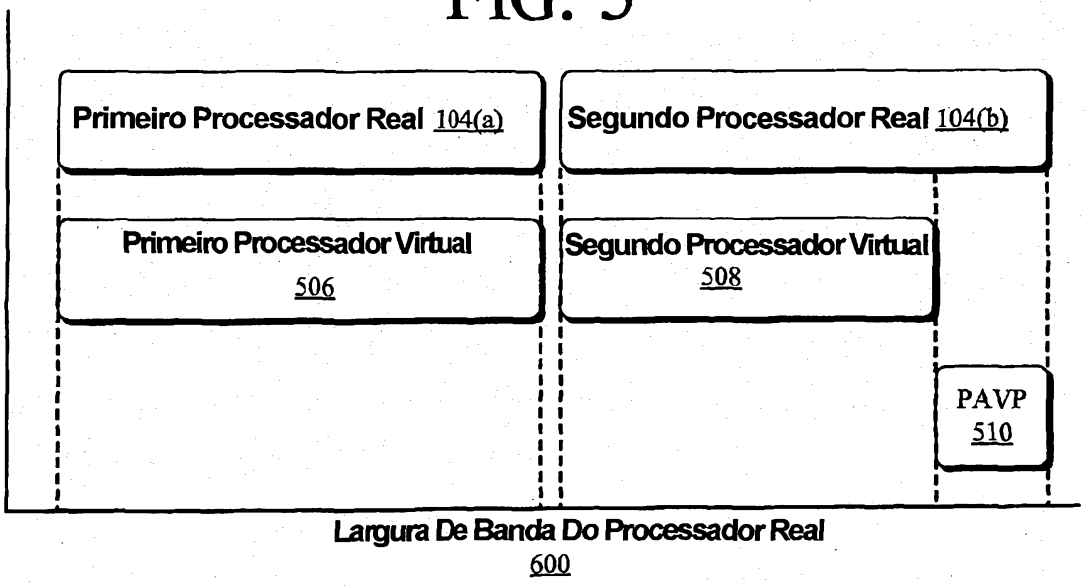
Primeiro Processador Real 104(a)
Segundo Processador Real 104(b)
Primeiro Processador Virtual
506
Segundo Processador Virtual
508
PAVP
510
Largura De Banda Do Processador Real
600

FIG. 6

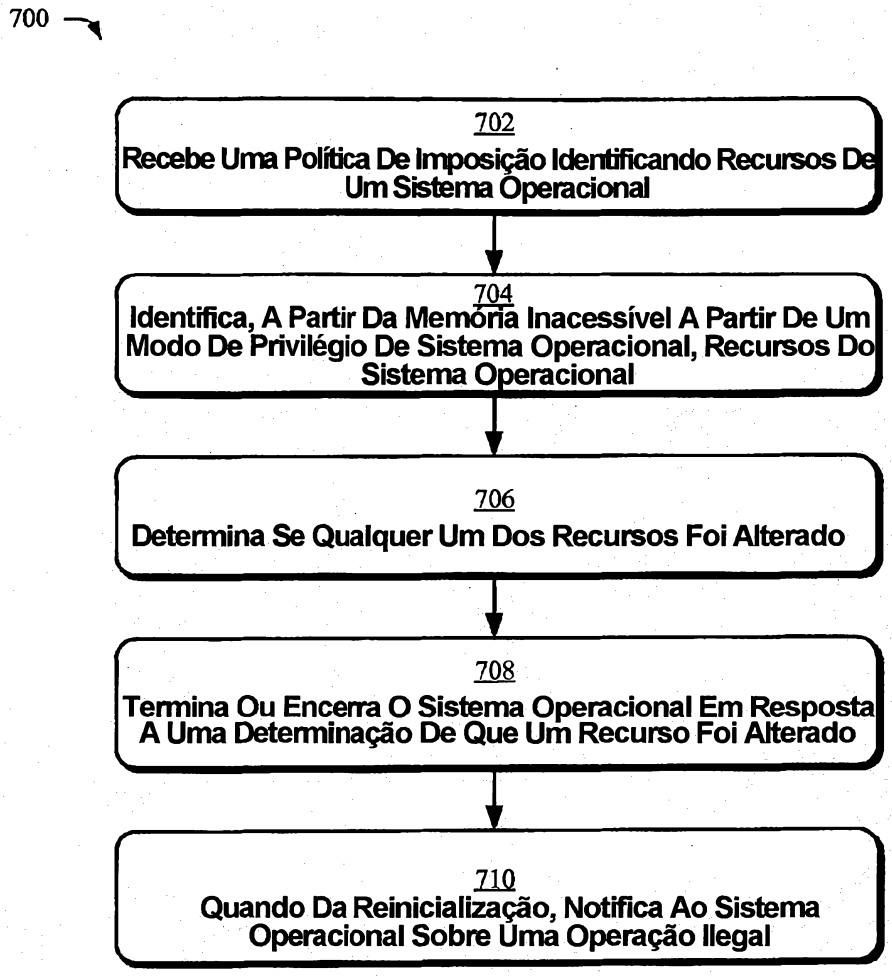
700
702
Recebe Uma Política De Imposição Identificando Recursos De Um Sistema Operacional
704
Identifica, A Partir Da Memória Inacessível A Partir De Um Modo De Privilégio De Sistema Operacional, Recursos Do Sistema Operacional
706
Determina Se Qualquer Um Dos Recursos Foi Alterado
708
Termina Ou Encerra O Sistema Operacional Em Resposta A Uma Determinação De Que Um Recurso Foi Alterado
710
Quando Da Reinicialização, Notifica Ao Sistema Operacional Sobre Uma Operação Ilegal

FIG. 7

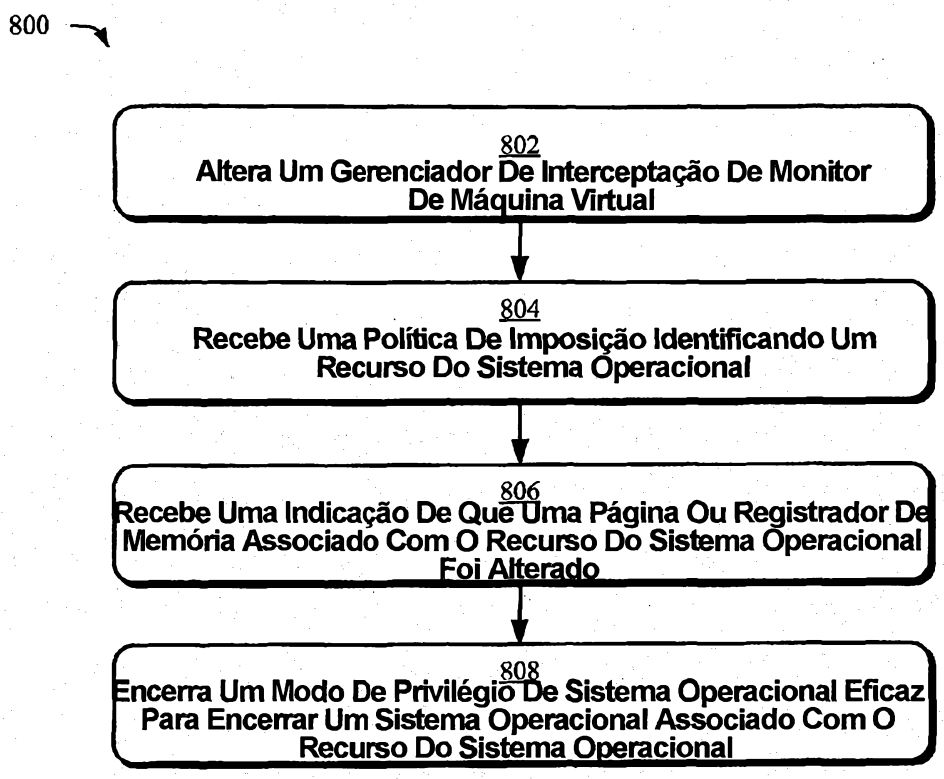
800
802
Altera Um Gerenciador De Interceptação De Monitor De Máquina Virtual
804
Recebe Uma Política De Imposição Identificando Um Recurso Do Sistema Operacional
806
Recebe Uma Indicação De Que Uma Página Ou Registrador De Memória Associado Com O Recurso Do Sistema Operacional Foi Alterado
808
Encerra Um Modo De Privilégio De Sistema Operacional Eficaz Para Encerrar Um Sistema Operacional Associado Com O Recurso Do Sistema Operacional

FIG. 8

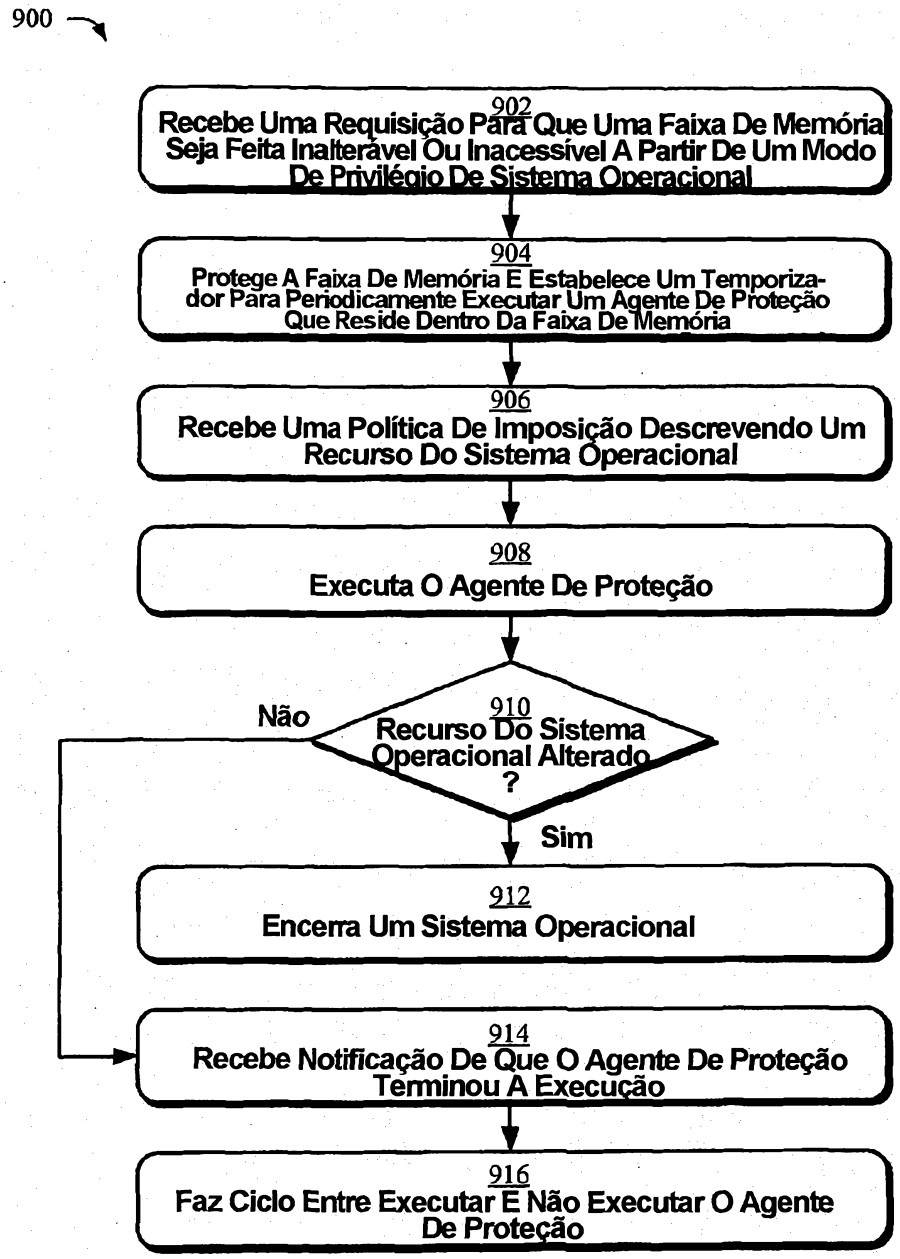
900
902
Recebe Uma Requisição Para Que Uma Faixa De Memória Seja Feita Inalterável Ou Inacessível A Partir De Um Modo De Privilégio De Sistema Operacional
904
Protege A Faixa De Memória E Estabelece Um Temporizador Para Periodicamente Executar Um Agente De Proteção Que Reside Dentro Da Faixa De Memória
906
Recebe Uma Política De Imposição Descrevendo Um Recurso Do Sistema Operacional
908
Executa O Agente De Proteção
910
Recurso Do Sistema Operacional Alterado ?
Não
Sim
912
Encerra Um Sistema Operacional
914
Recebe Notificação De Que O Agente De Proteção Terminou A Execução
916
Faz Ciclo Entre Executar E Não Executar O Agente De Proteção

FIG. 9

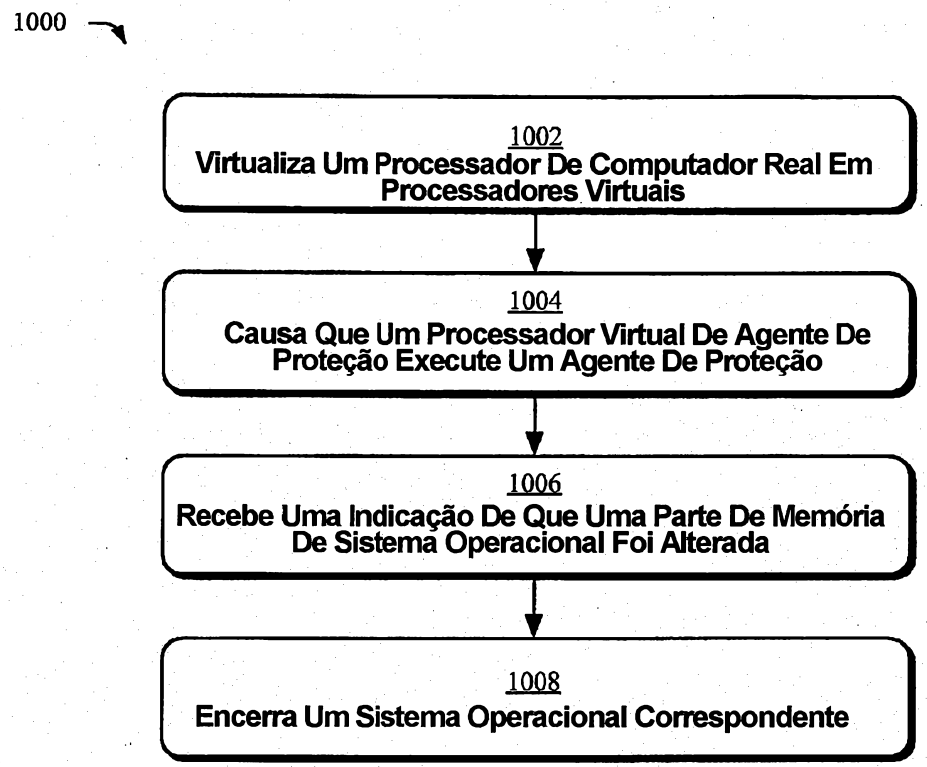
1000
1002
Virtualiza Um Processador De Computador Real Em Processadores Virtuais
1004
Causa Que Um Processador Virtual De Agente De Proteção Execute Um Agente De Proteção
1006
Recebe Uma Indicação De Que Uma Parte De Memória De Sistema Operacional Foi Alterada
1008
Encerra Um Sistema Operacional Correspondente

FIG. 10

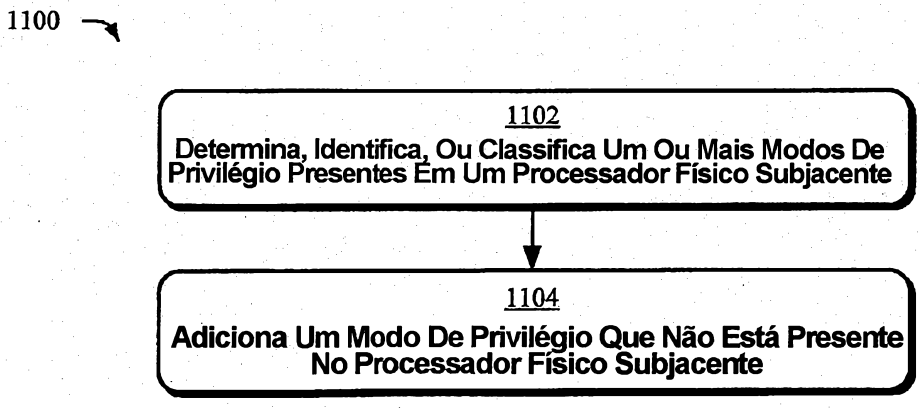
1100
1102
Determina, Identifica, Ou Classifica Um Ou Mais Modos De Privilégio Presentes Em Um Processador Físico Subjacente
1104
Adiciona Um Modo De Privilégio Que Não Está Presente No Processador Físico Subjacente

FIG. 11