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

(21) **PI 0713196-8 A2**

* B R P I 0 7 1 3 1 9 6 A 2 *

(22) Data de Depósito: 19/07/2007
(43) Data da Publicação: 20/03/2012
(RPI 2150)

(51) Int.Cl.:
G06F 21/04

(54) Título: SISTEMA DE AUTANTICAÇÃO DE UMA USUÁRIO VIRTUAL E MÉTODO DE AUTENTICAÇÃO DE UM USUÁRIO

(30) Prioridade Unionista: 25/07/2006 US 11/492,617

(73) Titular(es): HEWLETT-PACKARD DEVELOPMENT COMPANY, L.P.

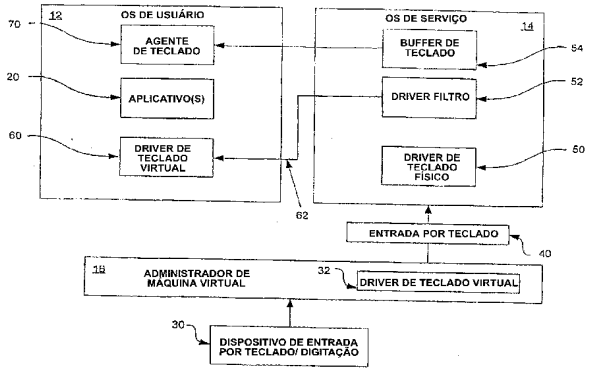
(72) Inventor(es): MANUEL NOVOA, MARK J. ALTENDORF, VALIUDDIN Y. ALI

(74) Procurador(es): ANTONIO MAURICIO PEDRAS ARNAUD

(86) Pedido Internacional: PCT US2007016410 de 19/07/2007

(87) Publicação Internacional: WO 2008/013738de 31/01/2008

(57) Resumo: SISTEMA DE AUTENTICAÇÃO DE UM USUÁRIO VIRTUAL E MÉTODO DE AUTENTICAÇÃO DE UM USUÁRIO VIRTUAL. Um sistema de autenticação de usuário virtual (10) compreende um administrador de máquina virtual (VMM) (16) comunicativamente acoplado a um Sistema Operacional de Usuário (OS) (12) e um OS de Serviço (14), o VMM (16) sendo configurado para receber as entradas por teclado destinadas a um aplicativo (20) em execução no OS de Usuário (12) e comunicar as entradas por teclado ao OS de Serviço (14), ademais as entradas por teclado são processadas pelo OS de Serviço (14).



PI0713196-8

"SISTEMA DE AUTENTICAÇÃO DE UM USUÁRIO VIRTUAL E MÉTODO DE AUTENTICAÇÃO DE UM USUÁRIO VIRTUAL".

Histórico da Invenção

Um usuário de plataforma usualmente é autenticado pela validação de uma ou mais credenciais associadas, (Nome, Senha, identificação ID (PIN), etc.). A informação de autenticação também pode ser usada em combinação com tokens criptográficos ou cartões inteligentes para combinar uma autenticação multi-fator para reforçar a segurança e autenticidade para o usuário. No entanto, há vários programas de escaneamento de memória e/ou copiadores de digitação. Assim, a credencial de segurança é suscetível de quebra (i.e., se usada para acessar um token criptográfico ou cartão inteligente de segurança).

Descrição Resumida dos Desenhos

Para um entendimento mais completo da presente invenção, e suas vantagens, se recorrem à descrição que se segue, em conexão com os desenhos anexos, nos quais:

A figura 1 é um diagrama que ilustra uma configuração de sistema de autenticação de um usuário virtual, de acordo com a presente invenção;

As figuras 2A e 2B são diagramas de fluxo que ilustra uma configuração de um método de autenticação de um usuário virtual, de acordo com a presente invenção; e

A figura 3 é um diagrama que ilustra outra configuração de um sistema de autenticação de usuário virtual, de acordo com a presente invenção.

Descrição Detalhada dos Desenhos

As configurações preferidas da invenção e suas vantagens serão melhor entendidas com referência às figuras 1 a 3, nos quais os mesmos número de referência se referem a partes iguais ou correspondentes nos vários desenhos.

A figura 1 é um diagrama que ilustra uma configuração de um sistema de autenticação de usuário virtual 10 de acordo com a invenção. Na configuração da figura 1, o sistema 10 compreende um Sistema Operacional de Usuário (OS de Usuário) 12, um Sistema Operacional de Serviço

(OS de Serviço) 14 e um Administrador de Máquina Virtual (VMM de "Virtual Machine Manager") 16. O VMM 16 compreende uma camada de software para tornar virtual a interface de hardware de OS de Usuário 12 e OS de Serviço 14 que é disposta em um espaço particionado de memória. Na configuração da figura 1, duas situações de Sistema Operacional são ilustradas, que são interfaceadas pelo VMM 16. No entanto, deve ser entendido que uma maior quantidade de Sistemas Operacionais é transformada em virtual usando VMM 16.

Na configuração da figura 1, o OS de Usuário 12 é configurado para ser o sistema operacional primário de um usuário de uma plataforma de computação para acessar e/ou de alguma forma usar Aplicativos 20, tal como, mas não se limitando a processadores de texto, navegador de Internet, e Financeiros. O OS de Serviço 14 é usado para processar as entradas por teclado recebidas a partir de um dispositivo de teclado 30 destinado a Aplicativos 20 (i.e. quais entradas são inseridas para prover informações para o Aplicativo 20). Por exemplo, o OS de Serviço 14 é configurado para interfacear com VMM 16 e com um agente de digitação 10 no OS de Usuário 12, para determinar se uma particular entrada por teclado for associada a uma credencial sensitiva de segurança para um certo Aplicativo 20 (Nome, Senha, Identificação (PIN), Seguridade Social, ou Informação confidencial). O OS de Serviço 14 processa as entradas por teclado correspondentes ao particular Aplicativo 20, e facilita a provisão das entradas por teclado para o particular Aplicativo 20, de modo que um copiador de digitação e/ou aplicativo de escaneamento associados e/ou integrados de alguma forma à pilha de protocolo de digitação/ teclado do OS de Usuário 12 não tenha acesso às entradas por teclado, daí melhorando a segurança de autenticação e/ou credencial de segurança.

Na configuração ilustrada na figura 1, o VVM compreende um driver de teclado virtual 32 que pode compreender

hardware, software, firmware, ou uma combinação destes. O driver de teclado virtual 32 é atuado pelo dispositivo de teclado 30 e comunica as entradas por teclado ao OS de Serviço 13 (as entradas do dispositivo de teclado 30 são identificadas na figura 1 como entrada por teclado 40). Assim, em operação, a entrada pelo dispositivo de teclado 30 para um Aplicativo 20 que reside, ou de alguma forma é executado no OS de Usuário 12, é interceptada por VMM 16, e em vez disso transmitida ao OS de Serviço 14.

Na figura 1, o OS de Serviço 14 compreende um driver de teclado físico 50, um driver filtro 52, e um buffer de teclado 54. O driver de teclado físico 50 e o driver filtro 52 podem compreender um software, hardware, firmware, ou uma combinação destes. O driver de teclado físico 50 recebe e/ou de alguma outra forma processa as entradas por teclado 40 recebidas a partir do VMM 16. O driver filtro 52 interfaceia um driver de teclado físico 50 e/ou Aplicativo 20 para determinar se as entradas por teclado 40 são associadas a uma credencial de segurança. Por exemplo, em algumas configurações da invenção, em resposta a uma ação de usuário e/ou de alguma outra forma executando um particular Aplicativo 20 e/ou uma função associada ao particular Aplicativo 20, o driver filtro 52 interfaceia o Aplicativo 20 para determinar se as entradas por teclado 40 são associadas à credencial de segurança para o Aplicativo 20 (i.e., em uma janela de entrada para Nome, Senha, ou um tipo de credencial de segurança). Se o driver filtro 52 determinar que as entradas por teclado 40 são associadas à credencial de segurança, o driver filtro 52 gera uma cadeia de caracteres arbitrários ou misturados de reserva de espaço ("spaceholder") correspondente aos caracteres que formam entradas por teclado 40. Por exemplo, se uma entrada por teclado 40 compreender senha BLD1359, o driver filtro 52 gera caracteres arbitrários para cada um dos caracteres da entrada por teclado 40. Assim, neste exemplo, o driver filtro 52 pode gerar uma cadeia de

caracteres definida como P**$&N2. Deve ser entendido que os caracteres arbitrários de reserva de espaço podem compreender uma pré-determinada cadeia de caracteres (por exemplo, tudo asteriscos) ou uma cadeia de caracteres gerados randomicamente.

Os caracteres arbitrários de reserva de espaço são transmitidos pelo driver filtro 52 a um driver de teclado virtual 60 associado ao OS de Usuário 12, como indicado pela seta 62 na figura 1. O driver de teclado virtual 60 recebe os caracteres arbitrários de reserva de espaço do driver filtro 52 e processa os caracteres arbitrários de reserva de espaço com a entrada por teclado 40. Por exemplo, o driver de teclado virtual 80 pode dispor os caracteres arbitrários de reserva de espaço em uma interface de usuário e/ou dispor dispositivo em uma janela de entrada correspondente ao Aplicativo 20. No entanto, deve ser entendido que pelo menos para a entrada por teclado 40 associada às credenciais de segurança, a entrada por teclado 40 não é recebida e/ou de alguma forma processada pelo driver de teclado virtual 60. Assim, um copiador e/ou escaneador de digitação afixado e/ou de alguma forma interfaceando o driver de teclado virtual 60, terá um acesso limitado, ou mesmo nenhum acesso, às entradas por teclado 40.

Preferivelmente, o driver filtro 52 também faz as entradas por teclado 40 serem armazenadas no buffer de teclado 54. Na figura 1, o agente de teclado 70 no OS de Usuário 12 que pode compreender hardware, software, firmware, ou uma combinação destes, interfaceia o driver filtro 52 e/ou o buffer de teclado 54, em resposta a um caractere de terminação ou entrada por teclado 40 recebida pelo OS de Serviço 14. Como usado aqui, o caractere de terminação da entrada por teclado 40 é geralmente definido como o caractere final ou último caractere de um particular entrada por teclado, seguido por um caractere (CR) "Retorno de Carro" padrão, ou quando um usuário sinaliza de outra forma (por exemplo,

tecla OK, etc. indicando o fim da entrada). Assim, por exemplo, para senha BLD1359, a terminação da entrada seria sinalizada como caractere "9" seguida pela seqüência "Retorno de Carro" (ENTER) ou invocando uma ação dentro do aplicativo (por exemplo, com botão OK). Em resposta ao recebimento do caractere de terminação da entrada por teclado 40, o agente de teclado 70 interfaceia o buffer de teclado 54 para automaticamente recuperar a entrada por teclado 40 do buffer de teclado 54 e prover a entrada por teclado 40 para o particular Aplicativo 20, ao qual se destina a entrada por teclado 40. Assim, neste exemplo, o período de tempo no qual a localização de memória pode ser escaneada de modo a determinar e/ou de alguma forma identificar uma credencial de segurança, é substancialmente reduzido. Neste exemplo, a entrada por teclado 40 é armazenada e/ou acumulada no buffer de teclado 54 até o caractere de terminação 40 poder ser processado, sem armazenar no buffer todos caracteres da entrada por teclado 40 antes de prover a entrada por teclado 40 ao Aplicativo 20 de destino. Por exemplo, em algumas configurações da invenção, o agente de teclado 70 pode ser configurado de modo a recuperar grupos de caracteres, ou mesmo um caractere individual, de entrada por teclado 40 em modo contínuo e/ou periódico, e prover esta entrada por teclado 40 ao Aplicativo 20 de destino.

Na configuração descrita, o driver filtro 52 gera caracteres arbitrários de reserva de espaço, se a entrada por teclado 40 for associada a uma credencial de segurança. No entanto, deve ser entendido que o driver filtro 52 pode ser configurado para gerar e transmitir ao driver de teclado virtual 60 caracteres arbitrários de reserva de espaço para todos tipos de entrada por teclado 40 (i.e., associada ou não a uma credencial de segurança). Ademais, deve ser entendido que, se a entrada por teclado 40 não for associada a uma credencial de segurança, a entrada por teclado 40 poderá ser

diretamente transmitida ao driver de teclado virtual 60 para processamento.

As figuras 2 e 2B são diagramas de blocos que ilustram a configuração de um método de autenticação de usuário virtual de acordo com a invenção. O método inicia no bloco 200, onde a entrada por teclado 40 é recebida no VMM 16. No bloco 202, o driver de teclado virtual 32 comunica as entradas por teclado 40 ao OS de Serviço 14. No bloco de decisão 204, é determinado se a entrada por teclado 40 é associada a uma credencial de segurança e/ou a um Aplicativo relativo à segurança 20. Se a entrada por teclado 40 não for associada a uma credencial de segurança e/ou a um Aplicativo relativo à segurança 20, o método avança para o bloco 206, onde o driver filtro 52 transmite e/ou de alguma outra forma comunica a entrada por teclado 40 ao driver de teclado virtual 60 do OS de Usuário 12. O método avança para o bloco 208, onde o driver de teclado virtual 60 provê a entrada por teclado 40 recebida ao Aplicativo 20, a que se destina.

Se no bloco de decisão 204 é determinado que a entrada por teclado 40 é associada a uma credencial de segurança e/ou a um Aplicativo 20 relativo à segurança, o método avança para o bloco 210, onde o driver filtro 52 gera caracteres arbitrários e/ou misturados de reserva de espaço. No bloco 212, o driver filtro 52 transmite e/ou de alguma outra forma comunica os caracteres de reserva de espaço ao driver de teclado virtual 62 do OS de Usuário 12. No bloco 214, o driver filtro 52 faz que a entrada por teclado 40 seja armazenada no buffer de teclado 54.

No bloco de decisão 204, determina-se se um caractere de terminação da entrada por teclado 40 para o Aplicativo 20 de destino inserido/ recebido. Se o caractere da entrada por teclado não tiver sido inserido/ recebido, o método avança para o bloco 214, onde a entrada por teclado 40 continua para ser armazenada no buffer de teclado 54. Se no bloco de decisão 216, for determinado que o

caractere de terminação da entrada por teclado 40 foi aplicado/ recebido, o método avança para o bloco 218, onde o agente de teclado 70 interfaceia com o buffer de teclado 54 para recuperar e/ou de alguma outra forma obter a entrada por teclado 40 a partir do buffer de teclado 54. No bloco 220, o agente de teclado 70 provê a entrada por teclado 40 recuperada do buffer 54 para o Aplicativo 20 a que se destina.

Na configuração ilustrada e descrita em conexão com as figuras 1, 2A, 2B, vários tipos de comunicações e/ou funções associadas ao processamento da entrada por teclado 40 são realizados diretamente entre o OS de Serviço 14 e o OS de Usuário 12 (i.e. comunicações entre e/ou acesso ao buffer de teclado 54 do OS de Serviço 14 por um agente de teclado 70 do OS de Usuário 12, comunicações entre o driver de filtro 52 do OS de Serviço 14, e driver de teclado virtual 60 do OS de Usuário 12, etc..). No entanto, deve ser entendido que vários tipos de comunicações e funções associadas a processamento da entrada por teclado 40 podem ser processados e/ou de alguma outra forma, comunicados entre o OS de Serviço 14 e o OS de Usuário 12 via VMM 16. Por exemplo, em algumas configurações da invenção, os caracteres arbitrários e/ou misturados de reserva de espaço gerados pelo driver filtro 52 seriam comunicados ao VMM 16 OS de Serviço 14, e o VMM 16 transmitiria os caracteres arbitrários e/ou misturados ao driver de teclado 60. Ademais, por exemplo, em algumas configurações, a entrada por teclado 40 armazenada no buffer 54 é transmitidas para o VMM 16, o qual interfaceia o agente de teclado 70 para facilitar a entrada por teclado 40 real para um certo Aplicativo 20. Assim, em algumas configurações, o VMM 16 atua como porteiro ou controlador de comunicação entre diferentes partições de OS, para processar a entrada por teclado 40.

A figura 3 é um diagrama que ilustra outra configuração de um sistema de autenticação de usuário virtual 10,

de acordo com a invenção. Na figura 3, ilustra-se o driver filtro 52 interfaceando e/ou se comunicando diretamente com o driver de teclado virtual 60, indicado pela seta 62, para transmitir caracteres arbitrários de reserva de espaço (i.e. para entrada de uma credencial de segurança) para o driver de teclado virtual 60. Na configuração ilustrada na figura 3, se a entrada por teclado não for associada à credencial de segurança, tal entrada de credencial de não-segurança é comunicada de volta para o VMM 16 a partir da OS de Serviço 14, como indicado pela seta 90, e provida para o OS de Usuário 12 pelo VMM, como indicado pela seta 92.

Assim, as configurações da invenção provêem um mecanismo de desvio (by pass) para processar as entradas por teclado, de modo que um copiador de digitação (keylogger) ou outros aplicativos copiadores de digitação alojados no Sistema Operacional (OS), ao qual se destinam as entradas por teclado (aplicativos executados no Sistema Operacional), tenham pouco ou mesmo nenhum acesso às entradas por teclado. Por exemplo, configurações do processo da presente invenção usam um administrador de máquina virtual para interceptar e processar a digitação por uma Plataforma ou Sistema Operacional diferente. Ademais, configurações da invenção armazenam as entradas por teclado no Sistema Operacional de desvio (by pass), até preferivelmente todas as entradas por teclado tiverem sido recebidas, em qual momento as entradas por teclado são recuperadas e carregadas no Aplicativo 20 a que se destinam, daí reduzindo grandemente o tempo de escanear um espaço de memória, buscando entradas por teclado.

REIVINDICAÇÕES

1- Sistema de autenticação de um usuário virtual, caracterizado pelo fato de compreender:

- um administrador de máquina virtual (VMM) (16) comunicativamente acoplado a um sistema operacional de usuário (OS) (12) e um OS de Serviço (14), o VMM (16) sendo configurado para receber as entradas por teclado destinadas a um Aplicativo (20) a ser executado no OS de Usuário (12) e para comunicar as entradas por teclado ao OS de Serviço (14), sendo que as entradas por teclado são processadas pelo OS de Serviço (14).

2- Sistema, de acordo com a reivindicação 1, caracterizado pelo fato de adicionalmente compreender um agente de teclado (70) disposto no OS de Usuário (12), sendo configurado para recuperar as entradas por teclado para o Aplicativo (20).

3- Sistema, de acordo com a reivindicação 1, caracterizado pelo fato de o OS de Serviço (14) ser configurado para determinar se as entradas por teclado são associadas a uma credencial sensitiva de segurança.

4- Sistema, de acordo com a reivindicação 1, caracterizado pelo fato de o OS de Serviço (114) ser configurado para gerar caracteres arbitrários de reserva de espaço que correspondam a caracteres de entradas por teclado, se as entradas por teclado forem associadas a uma credencial sensitiva de segurança.

5- Sistema, de acordo com a reivindicação 4, caracterizado pelo fato de os caracteres arbitrários de reserva de espaço serem comunicados a um driver de teclado virtual (60) do OS de Usuário (12).

6- Sistema, de acordo com a reivindicação 1, caracterizado pelo fato de adicionalmente compreender um agente de teclado (70) disposto no OS de Usuário (12) e configurado para, em resposta a uma determinação de inserção de um caractere de terminação associado às entradas por teclado, recuperar a entrada por teclado.

7- Método de autenticação de um usuário virtual,

caracterizado pelo fato de compreender:

- receber, em um administrador de máquina virtual (VMM) (16), as entradas por teclado para um Aplicativo (20) para execução no Sistema Operacional de Usuário (12);
- transmitir as entradas por teclado do VMM (16) ao OS de Serviço (14); e
- processar as entradas por teclado com o OS de Serviço (14).

8- Método, de acordo com a reivindicação 7, caracterizado pelo fato de adicionalmente compreender determinar com o OS de Serviço (14), se as entradas por teclado são associadas a uma credencial sensitiva de segurança.

9- Método, de acordo com a reivindicação 7, caracterizado pelo fato de adicionalmente compreender gerar, pelo OS de Serviço (14), caracteres arbitrários de reserva de espaço que correspondem a caracteres de entrada por teclado, se a entrada por teclado for associada a uma credencial de segurança.

10- Método, de acordo com a reivindicação 9, caracterizado pelo fato de adicionalmente compreender transmitir caracteres arbitrários de reserva de espaço a um driver de teclado virtual (60) do OS de Usuário (12).

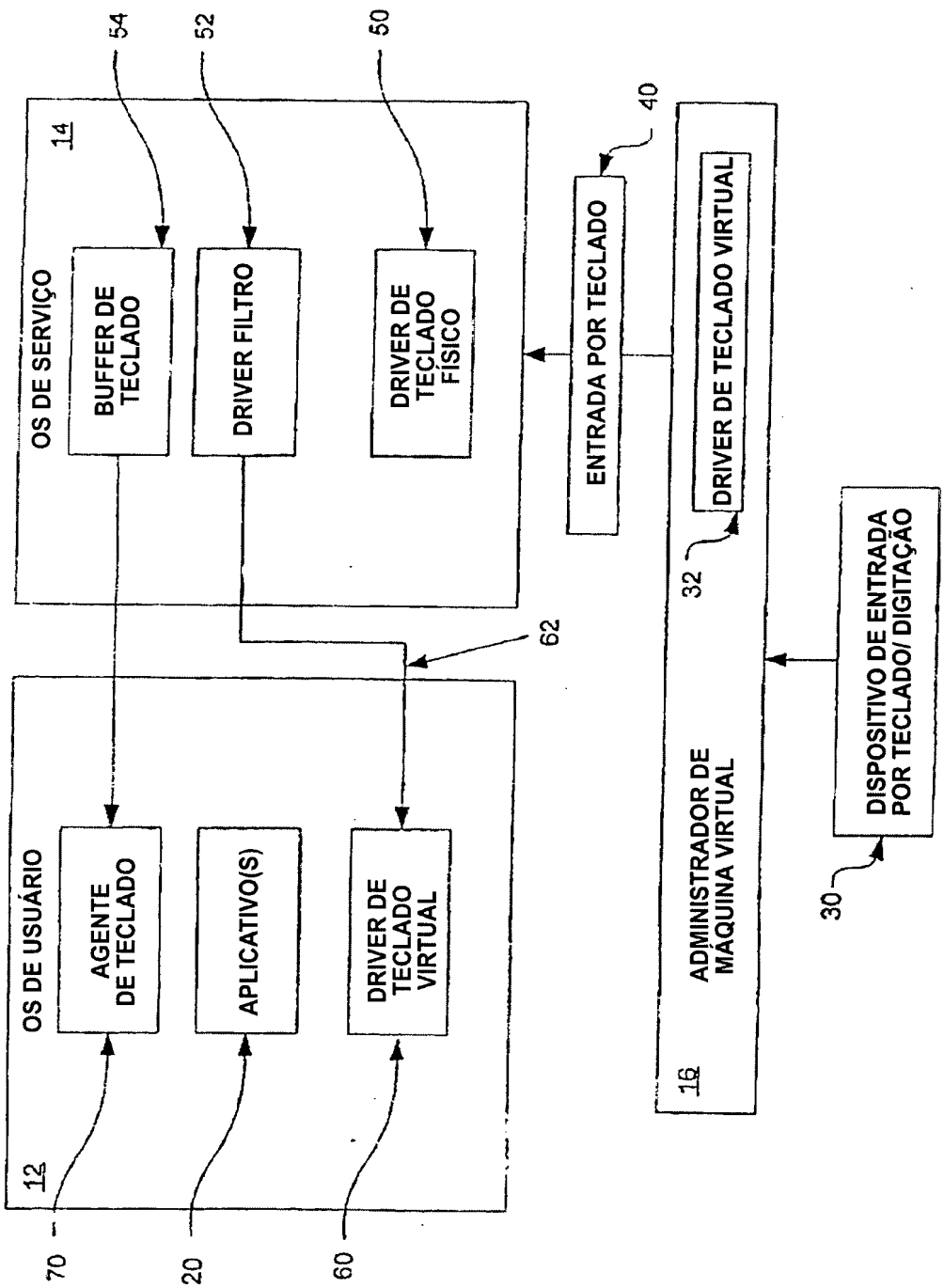

OS DE USUÁRIO
12
AGENTE DE TECLADO
APLICATIVO(S)
DRIVER DE TECLADO VIRTUAL
70
20
60
62
OS DE SERVIÇO
14
BUFFER DE TECLADO
DRIVER FILTRO
DRIVER DE TECLADO FÍSICO
54
52
50
ENTRADA POR TECLADO
40
ADMINISTRADOR DE MÁQUINA VIRTUAL
16
DRIVER DE TECLADO VIRTUAL
32
DISPOSITIVO DE ENTRADA POR TECLADO/ DIGITAÇÃO
30

FIG.1

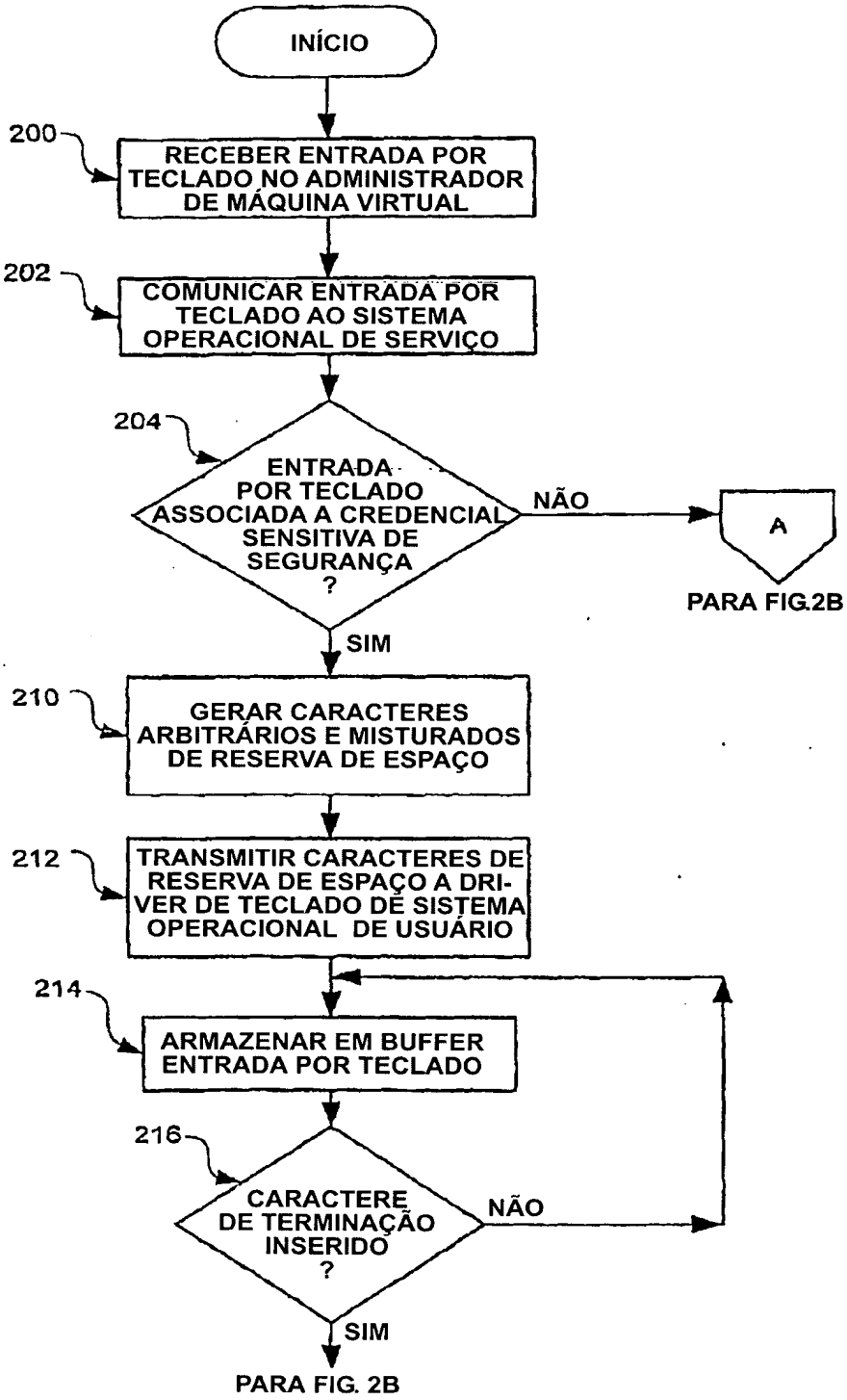

INÍCIO
200
RECEBER ENTRADA POR TECLADO NO ADMINISTRADOR DE MÁQUINA VIRTUAL
202
COMUNICAR ENTRADA POR TECLADO AO SISTEMA OPERACIONAL DE SERVIÇO
204
ENTRADA POR TECLADO ASSOCIADA A CREDENCIAL SENSITIVA DE SEGURANÇA ?
NÃO
A
PARA FIG.2B
SIM
210
GERAR CARACTERES ARBITRÁRIOS E MISTURADOS DE RESERVA DE ESPAÇO
212
TRANSMITIR CARACTERES DE RESERVA DE ESPAÇO A DRIVER DE TECLADO DE SISTEMA OPERACIONAL DE USUÁRIO
214
ARMAZENAR EM BUFFER ENTRADA POR TECLADO
216
CARACTERE DE TERMINAÇÃO INSERIDO ?
NÃO
SIM
PARA FIG. 2B

FIG.2A

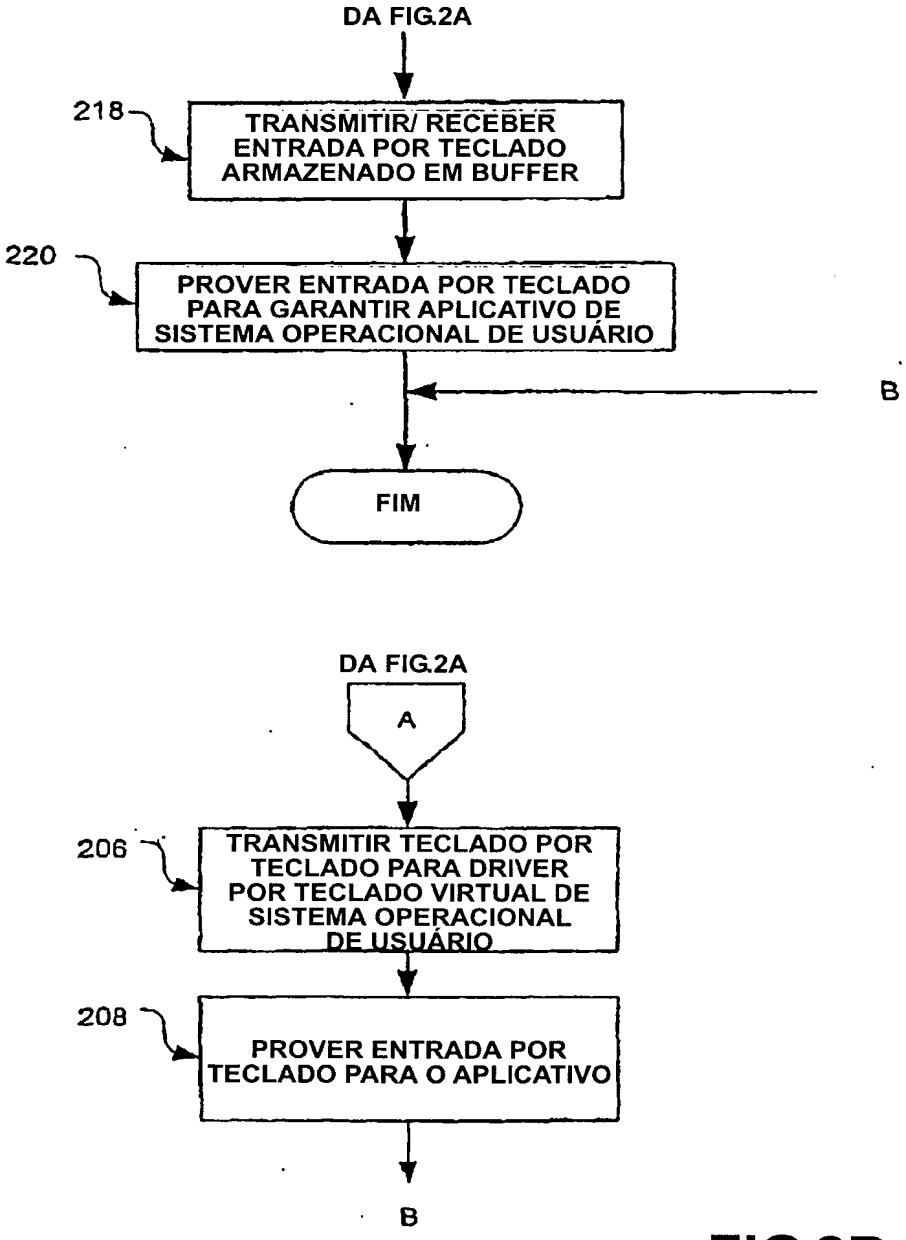

DA FIG.2A
218
TRANSMITIR/ RECEBER ENTRADA POR TECLADO ARMAZENADO EM BUFFER
220
PROVER ENTRADA POR TECLADO PARA GARANTIR APLICATIVO DE SISTEMA OPERACIONAL DE USUÁRIO
B
FIM
DA FIG.2A
A
206
TRANSMITIR TECLADO POR TECLADO PARA DRIVER POR TECLADO VIRTUAL DE SISTEMA OPERACIONAL DE USUÁRIO
208
PROVER ENTRADA POR TECLADO PARA O APLICATIVO
B

FIG.2B

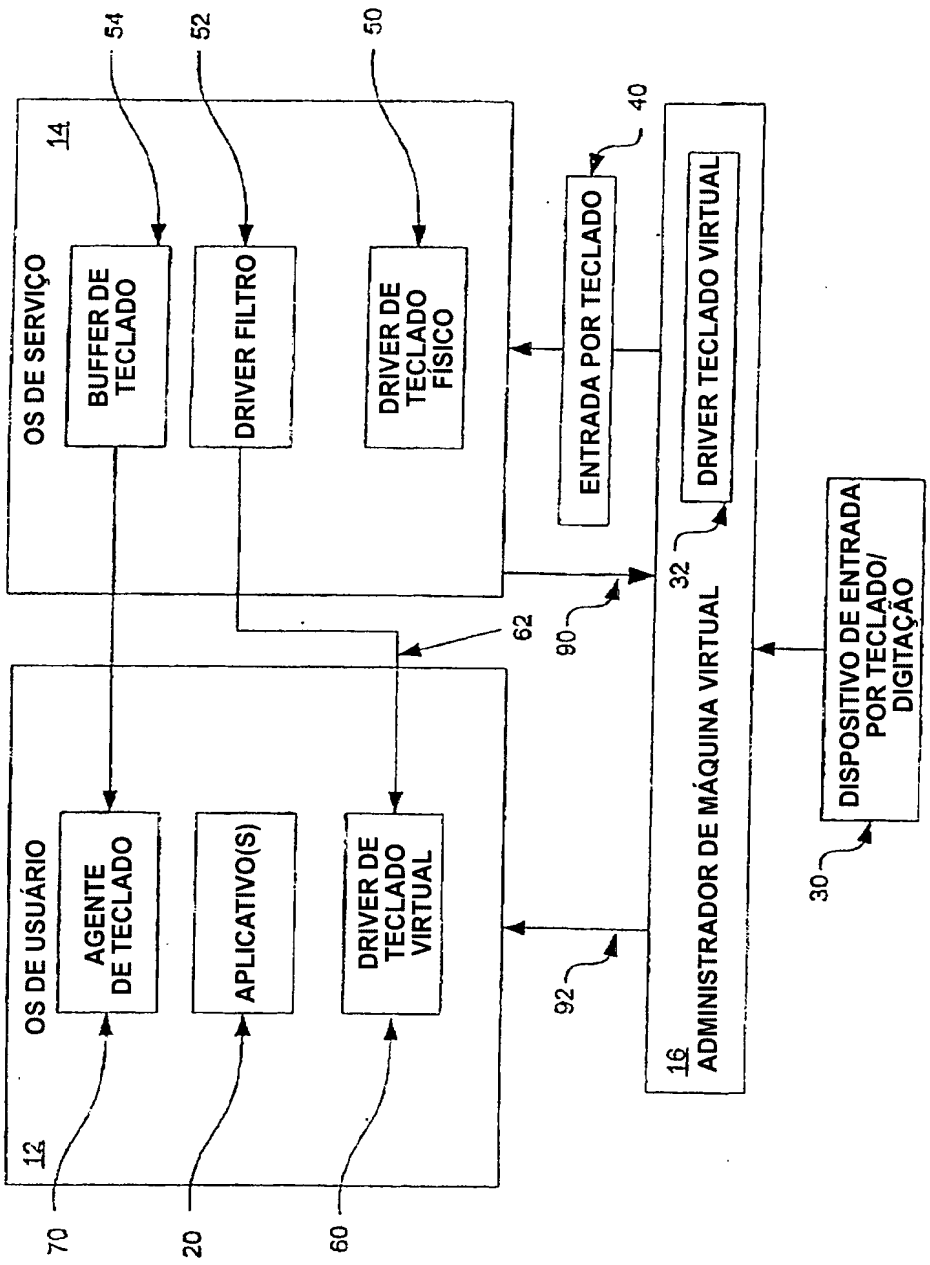

OS DE SERVIÇO
14
BUFFER DE TECLADO
DRIVER FILTRO
DRIVER DE TECLADO FÍSICO
54
52
50
ENTRADA POR TECLADO
40
DRIVER TECLADO VIRTUAL
32
ADMINISTRADOR DE MÁQUINA VIRTUAL
16
DISPOSITIVO DE ENTRADA POR TECLADO/ DIGITAÇÃO
30
62
90
92
OS DE USUÁRIO
12
AGENTE DE TECLADO
APLICATIVO(S)
DRIVER DE TECLADO VIRTUAL
70
20
60

FIG.3

RESUMO

"SISTEMA DE AUTENTICAÇÃO DE UM USUÁRIO VIRTUAL E MÉTODO DE AUTENTICAÇÃO DE UM USUÁRIO VIRTUAL".

Um sistema de autenticação de usuário virtual (10) compreende um administrador de máquina virtual (VMM) (16) comunicativamente acoplado a um Sistema Operacional de Usuário (OS) (12) e um OS de Serviço (14), o VMM (16) sendo configurado para receber as entradas por teclado destinadas a um aplicativo (20) em execução no OS de Usuário (12) e comunicar as entradas por teclado ao OS de Serviço (14), ademais as entradas por teclado são processadas pelo OS de Serviço (14).