República Federativa do Brasil
Ministério da Economia
Instituto Nacional da Propriedade Industrial

(11) BR 112015023183-7 B1

(22) Data do Depósito: 07/03/2014

(45) Data de Concessão: 05/04/2022

(54) Título: DISPOSITIVO, MÍDIA DE ARMAZENAMENTO LEGÍVEL POR COMPUTADOR E SERVIDOR PARA TESTES DE POSSE DE FATOR/CONHECIMENTO DE PRESERVAÇÃO DE PRIVACIDADE PARA AUTENTICAÇÃO PERSISTENTE

(51) Int.Cl.: G06F 21/30; G06F 15/16.

(30) Prioridade Unionista: 15/03/2013 US 13/844,619.

(73) Titular(es): GOOGLE LLC.

(72) Inventor(es): OMER BERKMAN; MARCEL M.M. YUNG.

(86) Pedido PCT: PCT US2014022075 de 07/03/2014

(87) Publicação PCT: WO 2014/150064 de 25/09/2014

(85) Data do Início da Fase Nacional: 14/09/2015

(57) Resumo: TESTES DE POSSE DE FATOR/CONHECIMENTO DE PRESERVAÇÃO DE PRIVACIDADE PARA AUTENTICAÇÃO PERSISTENTE As implantações exemplificativas descritas no presente documento são direcionadas à autenticação com base nos fatores privados do usuário, ao mesmo tempo em que não revelam no lado de servidor informações que permitam que o servidor (ou qualquer pes-soa com as informações do servidor) deduza as respostas privadas. Nas implantações exemplificativas, o usuário responde a um questionário com fatores de autenticação, em que as respostas são transformadas de maneira unidirecional e as respostas transforma-das são fornecidas ao lado de servidor. As implantações exemplificativas facilitam a autenticação com base na interpolação polinomial ou outros métodos para permitir que um usuário se autentique, mesmo que o usuário não responda a todas as perguntas correta-mente.

DISPOSITIVO, MÍDIA DE ARMAZENAMENTO LEGÍVEL POR COMPUTADOR E SERVIDOR PARA TESTES DE POSSE DE FATOR/CONHECIMENTO DE PRESERVAÇÃO DE PRIVACIDADE PARA AUTENTICAÇÃO PERSISTENTE

ANTECEDENTES

CAMPO DA TÉCNICA

[0001] Os aspectos das modalidades exemplificativas referem-se a testes de preservação de privacidade para uma autenticação persistente e, mais especificamente, a dispositivos, método e sistema para a geração de um hash de autenticação ou outra função unidirecional difícil de inverter e à autenticação com base no hash de autenticação gerado, de forma que as respostas a perguntas privadas não sejam reveladas no lado de servidor.

TÉCNICA RELACIONADA

[0002] Um usuário pode precisar provar sua identidade em várias situações durante um processo de autenticação de usuários para acesso e para recuperação de contas. Para facilitar a autenticação ou métodos alternativos para a autenticação (por exemplo, tolerância a falhas/recuperação), os usuários registram fatores (por exemplo, resposta a perguntas específicas à vida e ao gosto do usuário) no servidor que contém o acesso (por exemplo, provedor de conta). O registro por parte do usuário que inclui as respostas pode revelar informações privadas de usuário ao servidor. O acesso não autorizado ao servidor por parte de uma pessoa maliciosa pode revelar informações privadas de usuário a essa pessoa maliciosa. Por exemplo, essa pessoa (como alguém de dentro da organização do servidor ou alguém de fora ou um atacante de phishing) pode explorar as respostas registradas em outros provedores de conta ou no mesmo que podem exigir respostas similares e se fazer passar pelo usuário.

[0003] Para a autenticação, há uma necessidade de permitir que o usuário responda a perguntas (ou de fornecer outros fatores privados, tais como informações biométricas, informações possuídas armazenadas fora dos sistemas, etc.), enquanto, por questões de privacidade, o servidor não verifica as informações do usuário para conter as informações privadas.

SUMÁRIO

[0004] Os aspectos do presente pedido podem incluir um dispositivo, que envolve um processador, configurado para gerar uma pluralidade de hashes provenientes de uma pluralidade de respostas a uma pluralidade de perguntas; gerar um hash de autenticação a partir de pelo menos um de uma interpolação polinomial da pluralidade de hashes e uma seleção de um ou mais dentre a pluralidade de hashes para formar o hash de autenticação com base em um grupo selecionado dentre a pluralidade de perguntas; e autenticar com o hash de autenticação.

[0005] Os aspectos do presente pedido incluem adicionalmente uma mídia de armazenamento legível por computador que armazena instruções para executar um processo. As instruções podem envolver gerar uma pluralidade de hashes provenientes de uma pluralidade de respostas a uma pluralidade de perguntas; gerar um hash de autenticação a partir de pelo menos um dentre: uma interpolação polinomial da pluralidade de hashes e uma seleção de um ou mais dentre a pluralidade de hashes para formar o hash de autenticação com base em um grupo selecionado dentre a pluralidade de perguntas; e autenticar com o hash de autenticação.

[0006] Os aspectos do presente pedido incluem adicionalmente um servidor, que pode incluir um processador configurado para transmitir uma pluralidade de perguntas; conceder acesso quando um hash de autenticação responsivo à pluralidade de perguntas transmitida corresponder a um hash de autenticação secreto; e negar acesso quando o hash de autenticação não corresponder ao hash de autenticação secreto; em que o hash de autenticação é gerado a partir de pelo menos um dentre: uma interpolação polinomial da pluralidade de hashes e uma seleção de um ou mais dentre a pluralidade de hashes para formar o hash de autenticação com base em um grupo selecionado dentre a pluralidade de perguntas.

BREVE DESCRIÇÃO DOS DESENHOS

[0007] As Figuras 1(a) e 1(b) ilustram um fluxograma para um dispositivo, de acordo com uma implantação exemplificativa.

[0008] As Figuras 2(a) e 2(b) ilustram um fluxograma para um servidor, de acordo com uma implantação exemplificativa.

[0009] A Figura 3 ilustra um ambiente de computação exemplificativo com um dispositivo de computação exemplificativo adequado para uso em algumas implantações exemplificativas.

[0010] A Figura 4 ilustra um ambiente de processamento exemplificativo de acordo com a implantação exemplificativa.

DESCRIÇÃO DETALHADA

[0011] A matéria descrita no presente documento é ensinada por meio de implantações exemplificativas. Vários detalhes foram omitidos a título de clareza e para evitar obscurecer a matéria. Os exemplos mostrados abaixo são direcionados a estruturas e funções para implantar a medição do desempenho de campanha com preservação da privacidade. Os aspectos das implantações exemplificativas podem se referir a comércio eletrônico, compartilhamento de informações, métodos de preservação de privacidade, criptografia e metodologias criptográficas, sistemas de transação, compartilhamento de informações privadas e computação segura, por exemplo. No entanto, as implantações exemplificativas não são limitadas aos mesmos e pode ser aplicadas a outros campos, sem se afastar do escopo do presente conceito inventivo.

[0012] As implantações exemplificativas descritas no presente documento são direcionadas à autenticação com base nos fatores privados do usuário, ao mesmo tempo não revelando no lado de servidor informações que permitam que o servidor (ou qualquer pessoa com as informações do servidor) deduza as respostas privadas. Nas implantações exemplificativas, o usuário responde a um questionário com fatores de autenticação, em que as respostas são transformadas de maneira unidirecional e as respostas transformadas são fornecidas ao lado de servidor. Isso protege a privacidade do usuário enquanto permite que o servidor autentique o usuário original que registrou as informações no servidor.

[0013] As implantações exemplificativas são direcionadas a permitir que uma pluralidade de fatores com entropia suficiente (por exemplo, cadeias de caracteres) sejam transformadas juntas no dispositivo de usuário sob uma função unidirecional (por exemplo, hash criptográfico) e a transmitir os valores transformados ao servidor

no registro. Em uma sessão de autenticação, pede-se as respostas novamente ao usuário, que são transformadas pelo dispositivo de maneira similar à descrita acima e enviadas ao servidor. O servidor, então, compara as respostas unidirecionais transformadas com as informações registradas. A descrição a seguir é direcionada a programas/protocolo mais detalhados que delineiam os mecanismos usados nas implantações exemplificativas.

[0014] A entidades de protocolo para implantações exemplificativas podem incluir um usuário, um dispositivo de usuário e um servidor. A título de clareza, os parâmetros de protocolo são expressados como n, t, r e m, os quais são descritos abaixo.

[0015] Em um ambiente de protocolo exemplificativo, há vários aspectos que devem ser considerados, conforme descrito abaixo.

[0016] Informações de registro privadas: O usuário tem cadeias de caracteres de informações privadas identificadas como n. Essas pode ser algo que o usuário sabe e tem chances de lembrar ou fatores que o usuário detém ou de outro modo possui. Nas implantações exemplificativas, o registro inicial pode ser validado, por exemplo, após o usuário receber e responder a um reconhecimento enviado a um dispositivo associado ao usuário (por exemplo, o telefone do usuário e uma conta associada ao usuário, tal como um e-mail alternativo ou uma conta de um amigo).

[0017] Identificação não privada: As identificações, o formato, possivelmente dicas, e a ordem das cadeias de caracteres não são privados.

[0018] Persistência: Em qualquer determinado momento, o usuário conhece pelo menos cadeias de caracteres n a t. Isto é, o usuário pode ter registrado cadeias de caracteres n, e não se pode presumir que o mesmo sempre se lembre de todas, podendo inclusive se esquecer de t das mesmas. Assim, exige-se que o usuário saiba um limite de n a t das cadeias de caracteres. Observe-se que o nível exigido pode ser ajustado pelo servidor de uma sessão de autenticação para a outra.

[0019] Dispositivo de usuário: O usuário tem acesso a um dispositivo que pode inserir dados de modo seguro, computar, apagar dados, salvar dados e emitir dados. O dispositivo fica sob o controle do usuário (por exemplo, não é passível de

phishing). Esse pode ser um dispositivo tipo smartphone ou um elemento de software que não seja conectado à Web.

[0020] Integridade parcial de dispositivo: O dispositivo opera corretamente (em particular, os dados são permanentemente apagados quando solicitado), mas pode ser perdido/roubado.

[0021] Integridade de servidor: o servidor opera corretamente e nunca perde quaisquer dados, visto que o servidor está interessado em autenticar o usuário. Adicionalmente, os dados armazenados a longo prazo no servidor não contêm dados que permitam que os atacantes se façam passar por um usuário.

[0022] Configuração: Durante a configuração, o dispositivo e o servidor podem trocar informações de modo seguro.

[0023] O ambiente de protocolo exemplificativo pode também incluir vários requisitos, tais como:

[0024] Privacidade: Considerando o conhecimento de r das cadeias de caracteres privadas, as informações no servidor, no dispositivo ou as informações trocadas entre o servidor e o dispositivo devem ser substancialmente insuficientes para revelar qualquer uma dentre as cadeias de caracteres n a r restantes ou para se adivinhar melhor do que inicialmente qualquer uma dentre as cadeias de caracteres n a r restantes.

[0025] Autenticidade: A qualquer momento, o usuário pode provar ao servidor (com o uso do dispositivo) que o usuário sabe pelo menos n a t das cadeias de caracteres inseridas (n a t é bem maior do que r). Essa operação de autenticidade determina um resultado bem-sucedido da operação, e o servidor pode mudar o limite n a t necessário de forma possivelmente dinâmica em várias sessões de autenticação.

[0026] Segurança: As informações no servidor, no dispositivo enquanto não usado pelo usuário ou as informações trocadas entre o servidor e o dispositivo devem ser substancialmente insuficientes para serem usadas para autenticar um usuário que pode não ser o usuário original que se registrou inicialmente.

[0027] O ambiente de protocolo exemplificativo pode empregar vários protocolos.

Por exemplo, o registro de fator pode ser realizado para configurar vários fatores. O registro de fator pode envolver aleatorização, tabulação, resposta e geração.

[0028] No aspecto de aleatorização do registro de fator, o dispositivo e o servidor podem, juntos, gerar aleatoriedade com um gerador de número aleatório ou outros métodos. Em uma implantação exemplificativa, o servidor fornece um Rs de sal aleatório longo (não secreto) ao dispositivo. O usuário pode gerar um Ru de sal aleatório longo (não secreto) e inserir Rs e Ru no dispositivo. O dispositivo gera um Rd de sal aleatório longo (não secreto) e concatena todos os três sais aleatórios em um único R de sal aleatório (R de sal pode ser um fator a ser empregado pelo servidor em interações adicionais).

[0029] No aspecto de tabulação do registro de fator, o provisionamento de identificação pode ser realizado. O servidor fornece ao usuário um conjunto de identificações de cadeia de caracteres e os respectivos possíveis formatos de cada cadeia de caracteres e um conjunto de “dicas” padrão a ser empregado pelo usuário. A identificação é uma variável para a qual o usuário fornece um valor que está em uma cadeia de caracteres em um determinado formato. O usuário pode escolher identificações n a partir do conjunto de identificações ordenado oferecido para definir o questionário. Nas implantações exemplificativas, alguns elementos no questionário podem não necessariamente ser do tipo “algo que você sabe”, e outros tipos de informações (por exemplo, biométrica, perguntas personalizadas, etc.) podem também ser usados.

[0030] No aspecto de resposta do registro de fator, o usuário fornece respostas de questionário como cadeias de caracteres n. O usuário pode ser treinado pelo sistema para repetir as respostas como parte do processo (por exemplo, pergunta-se ao usuário duas vezes, o sistema emprega técnicas para aumentar a memória do usuário sobre as respostas, etc.). As respostas podem ser movidas ao dispositivo.

[0031] O questionário pode ser mantido em segredo ou pode ser misturado com outros métodos que são abertos (por exemplo, o servidor sabe respostas diretas), dependendo da implantação desejada. Por exemplo, o questionário pode ser usado em combinação com outros métodos de autenticação, (por exemplo, como melhorar

a reivindicação de identidade em vez de ser o único método.) Por exemplo, a combinação pode ser usada mediante a falha de outros métodos, após algum sucesso inicial com outros métodos, antes de outros métodos serem usados, somente quando o usuário já estiver autenticado mas solicitar acesso/ação sensível adicional.

[0032] No aspecto de geração de fator do registro de fator, o sistema gera os fatores para lembrar com base nas respostas e utilizando um algoritmo. Para inicializar o algoritmo, é fornecido ao dispositivo n segredos de usuário u_1, ..., u_n, em que u_i= a pergunta q_i e a resposta a_i. O dispositivo gera n segredos s_1, ..., s_n, que são um uma função de hash ou unidirecional do q_i' s. s_i=HASH(a_i, R). O dispositivo dos pontos (q_i, s_i) para i=1,n pode ser gerado por interpolação sobre um campo finito de um polinomial P de grau n-1 que atravessa todos pontos no plano. Cada um dentre q_i e s_i é interpretado no campo finito, por exemplo, o hash pode ser uma cadeia de caracteres de 256 bits interpretada com relação a um número primo de tamanho de 256 bits como elementos no campo finito definidos pelo número primo, q_1 e s_i gerados por meio de hashing têm probabilidade de ser mapeados a um ponto de aparência aleatória que pode ser visto como um ponto posicionado no plano cartesiano com coordenadas X e Y no campo finito. Campos finitos, números primos e interpolações polinomiais são noções básicas para o indivíduo versado na técnica. O segredo s é o valor da polinomial em 0 (isto é, P(0)=s), e pode ser registrado no servidor com um número de série. Além disso, pontos k=2t adicionais na polinomial, como os pontos (1, P(1)), (2,P(2)),… (k, P(k)) são enviados e registrados no servidor presumindo-se que esses não estão nos pontos originalmente usados na interpolação. Isso é para permitir que o usuário esteja errado ou omita possivelmente t das cadeias de caracteres n em uma futura autenticação. O polinomial P tem grau n-1 (visto que foi gerado por pontos n), e o registro do segredo que é o ponto (o, P(0)) e os pontos k adicionais deve ser que k+1 é menor do que n, e esse conhecimento de pontos k+1 não fornece ao servidor as propriedades polinomiais. Por exemplo, se for pedido ao usuário para o mesmo responder sobre 20 fatores, enquanto se reserva um limite de se exigir somente 15

respostas no futuro, então dez pontos são enviados ao servidor além do segredo. Quando um usuário autentica no futuro (a ser descrito abaixo como uma implantação exemplificativa), o usuário envia os fatores novamente e os 10 pontos adicionais são adicionados à representação da polinomial, e a interpolação ruidosa pode ser tentada pelo usuário, o que inclui esses pontos. Se um atacante tenta se fazer passar pelo usuário, o atacante saberá sempre menos do que dez pontos visto que os fatores foram cuidadosamente escolhidos para representar o conhecimento e a posse de fatores do usuário. Assim, os pontos enviados pelo servidor e o conhecimento de um imitador em tentativa falharão em interpolar os pontos disponíveis para recuperar a polinomial P.

[0033] Em outra implantação exemplificativa, o HASH(s) é mantido localmente em vez do próprio s. As outras informações podem ser deletadas ou mantidas pelo dispositivo, ou os pontos k serem mantidos no servidor, dependendo da implantação desejada. Por exemplo, apagar as outras informações força o usuário a inserir as informações novamente na autenticação, enquanto manter as informações pode ser usado para fornecer a posse do dispositivo. O HASH pode ser qualquer função unidirecional, um algoritmo de hash criptográfico ou uma exponenciação com um gerador sobre algum campo finito ou outra estrutura algébrica como conhecido para exponenciação modular na literatura criptográfica. Manter o HASH(s) em vez do s no servidor impede que atacantes que penetram no servidor aprendam o próprio s.

[0034] Em uma implantação exemplificativa, uma sessão de autenticação pode ser empregada conforme descrito abaixo. A sessão de autenticação pode incluir vários modos de uso dos fatores. Em um primeiro modo, o dispositivo está disponível, o usuário tem acesso ao dispositivo e o s secreto não foi deletado. No primeiro modo, o dispositivo, então, informa o servidor sobre o número de série do hash e prova conhecimento sobre o segredo usando um protocolo seguro.

[0035] Em um segundo modo de uso, o servidor, o usuário e o dispositivo (ou outro dispositivo) colaborativamente geram um dos hashes. O servidor envia ao usuário as identificações n (perguntas) e o formato das mesmas. Então, o servidor envia ao dispositivo as identificações n, e o R sal. O usuário insere no dispositivo a_i

as respostas. O servidor também envia os pontos k adicionais (1,P(1)),… (k,P(k)). Com o uso de um algoritmo de interpolação ruidosa (por exemplo, Berlekamp Welch, Guruswami-Sudan, etc.), o dispositivo computa a polinomial e, se um limite de respostas estiver correto (por exemplo, 2/3 como no exemplo de 15 dentre 20 acima, metade, etc.), o algoritmo de interpolação ruidosa produz s. Se o dispositivo tem HASH(s), o s produzido pode verificar a correção e pode pedir ao usuário novas respostas (por exemplo, se incorretas, pedir a inicialização, etc.). O s resultante é enviado ao servidor, em que o servidor autentica o usuário ou, alternativamente, o dispositivo do usuário prova a posse de s com base no HASH(s) que é enviado ao servidor, e, com essa finalidade, protocolos de zero conhecimento ou protocolos de resposta-desafio conhecidos na técnica podem ser utilizados.

[0036] Se um dentre os pontos para o algoritmo de interpolação ruidosa for um aleatorizador (por exemplo, contribuído pelo servidor ou software local), então o fator resultante é aleatorizado (isto é, independente das respostas do usuário). Por exemplo, assuma inicialmente que os ⅔ ligados do algoritmo de interpolação ruidosa Berlekamp Welch podem ser ajustados fazendo-se com que o servidor contribua com alguns pontos. Se um limite mais alto for desejado, então o servidor pode contribuir com pontos de erro (não na polinomial). Portanto, se o limite desejado for, por exemplo, 16 dentre 18 (16/18) pontos e o algoritmo de interpolação ruidosa Berlekamp Welch for empregado, seis erros podem ser introduzidos tanto pelo servidor quanto pelo dispositivo de modo que 16/24 pontos estejam corretos, chegando, assim, ao limite Berlekamp Welch. Em outro exemplo, se o limite implantado exigir que somente metade das respostas estejam corretas, então “bons pontos polinomiais” podem ser introduzidos pelo servidor ou pelo dispositivo. Por exemplo, se 10/18 (acima da metade das perguntas estiverem certas) for considerado suficiente, seis bons pontos podem ser introduzidos de forma que o resultado seja 16/24, o que chega ao limite Berlekamp Welch de 2/3. O ajuste do limite exigido pode variar de uma sessão de autenticação para a outra.

[0037] Devido ao fato de as informações escolhidas serem tão privadas, o usuário deve ter capacidade para relembrar quase todas as informações. A

complexidade é a da avaliação de uma polinomial em um campo finito.

[0038] As cadeias de caracteres podem ser bem privadas e envolver informações secretas que assegurem que o usuário possa relembrar a maior parte das mesmas quando exigido. Exemplos incluem nomes de irmãos, de crianças, cônjuges, pais, avôs, amigos, endereços próprios e de parentes, nomes e/ou números de conta, nome de empregadores e outros, dependendo da implantação desejada. Os critérios de seleção para as cadeias de caracteres devem ser de forma que o usuário tenha capacidade para recriar as respostas se necessário. A quantidade e a variabilidade dos dados devem ser de tal forma que cadeias de caracteres suficientes nunca sejam conhecidas por um atacante de modo que, mesmo com pontos extra provenientes do servidor, o atacante não possa produzir bons pontos de interpolação e a polinomial permaneça secreta ao atacante.

[0039] Em implantações exemplificativas, vários níveis de segurança podem também ser introduzidos. Por exemplo, as próprias identificações, formatação e ordem das cadeias de caracteres podem ser protegidas por algumas cadeias de caracteres básicas e fáceis de lembrar (por exemplo, senha do usuário)

[0040] A título de recuperação de conta e liberação de contas tomadas por sequestradores, deve ser empregado um fator de autenticação que é usado para o processo de recuperação e tem as seguintes propriedades:

[0041] Persistente: sempre disponível ao usuário; usuário não pode perder o mesmo (ou pode recriar) ainda que ele/ela perca um objeto físico que contenha o fator ou perca sua conta (por exemplo, por sequestro).

[0042] Não falsificável: substancialmente impossível de adivinhar mesmo quando é dado acesso à conta ou às informações pessoais de usuário. Deve ser não falsificável tanto por atacantes aleatórios quanto por associados do usuário.

[0043] Privado: não revela dados pessoais ao provedor de conta ou a um atacante; e

[0044] Disponível: implantável em sistemas de software gerais sem dispositivos com finalidade específica.

[0045] Existem várias considerações para se selecionar fatores. Por exemplo, se

o fator persistente for “algo que o usuário tem”, o usuário pode perder o fator ou o fator pode chegar às mãos do atacante. Se o fator persistente for “algo que o usuário conhece”, o fator pode não ser privado para o sistema verificar, e o usuário pode esquecer o fator. Se o fator persistente for “algo que o usuário é”, o fator exigirá algum reconhecimento de recurso humano (dispositivos biométricos, etc.) e pode não ser prontamente disponível e pode também revelar informações pessoais ao provedor.

[0046] Em implantações exemplificativas, fatores persistentes são utilizados com base no conhecimento de usuário (“algo que você sabe”) e podem também se basear em algo que o usuário possui. Tais requisitos podem ser difíceis de preencher com muitas das situações existentes. Portanto, as implantações exemplificativas podem envolver uma solução com base no conhecimento de usuário, presumindo-se que o usuário pode lembrar muitas perguntas básicas de modo confiável e emarando-se as respostas com operações criptográficas.

[0047] Conhecimento Próprio e de Outras Pessoas: Embora as implantações exemplificativas tenham se apresentado como baseadas no “conhecimento de usuário”, o conhecimento pode ser adquirido a partir de fiduciários e outras fontes em tempo real, e o acúmulo de conhecimento pode representar o conhecimento pessoal do usuário e o acesso do usuário a fiduciários. Os fiduciários podem representar parte do conhecimento sobre o usuário e ajudar o mesmo a produzir os fatores necessários.

[0048] As implantações exemplificativas podem envolver um processo básico para recuperação emergencial de acesso à conta, mas podem também ser implantadas como um método de autenticação geral que equilibra privacidade e autenticidade e leva a usabilidade em consideração (por exemplo, treinamento de usuário e interfaces de usuário para treinar o usuário quando o fator for necessário).

[0049] As contas que os usuários têm do provedor de conta de Internet estão ganhando importância à medida que os usuários mantêm seu e-mail, seus pagamentos eletrônicos, seu conteúdo pessoal, etc., na conta. Essas contas são importantes recursos pessoais e são suscetíveis a atacantes. As implantações

exemplificativas são direcionadas a sistemas e métodos de forma que o usuário possa reter e reivindicar a conta de um modo que um sequestrador não possa, se o usuário tiver um fator persistente de autenticação que esteja sempre disponível ao usuário e nunca ao atacante. Aproximar tal fator pode facilitar o processo de recuperação.

[0050] É o caso em que, na técnica relacionada, quando uma conta como uma conta de e-mail é sequestrada, um atacante tem o estado da conta e pode manipular a conta de modo que a recuperação pelo detentor não malicioso da conta que é o usuário possa ser mais difícil. O atacante pode também aprender a partir de todos os dados armazenados na conta. As implantações exemplificativas, portanto, utilizam mecanismos que não podem ser inferidos tendo-se acesso à conta. Similarmente, os mecanismos devem ser de tal forma que não possam ser perdidos se a conta não estiver disponível (por exemplo, sequestrados). A recuperação é, então, dominada pelo detentor dos fatores persistentes.

[0051] As implantações exemplificativas empregam uma fonte de conhecimento de usuário de alta entropia ou conhecimento que o usuário pode recriar quando necessário. Com tal propósito, uma grande quantidade de informações bem privadas de usuário é utilizada - nomes de irmãos, crianças, cônjuge, pais, avôs, amigos, endereço próprio e de parentes, nomes e/ou números de conta, nome de empregadores e mais. As informações devem ser de tal forma que o usuário possa recriar as respostas se necessário, e a quantidade e a variabilidade dos dados são de forma que bits suficientes nunca sejam conhecidos por um atacante. Similarmente, presume-se que outros fatores, como leitura biométrica ou acesso a fiduciários, como servidores de banco, também estejam em combinação, não conhecidos pelo atacante.

[0052] Em outra implantação exemplificativa, o fator pode ser gerado por um processo que tem entrada, processamento e saída para geração e para verificação do fator. O processo pode envolver entrada de usuário, entrada de sistema e uma computação criptográfica, em que cada um tem um papel.

[0053] A entrada pode envolver uma fonte de conhecimento de alta entropia, tal

como um conjunto de perguntas feitas ao usuário é Q1, Q2, Q3, etc., e as respostas: A1, A2, A3, etc. As respostas A1 devem ser de forma que o usuário possa lembrar (as perguntas podem ser feitas um número de vezes, e o usuário pode, assim, ser treinado para responder as mesmas). A escolha de tais perguntas pode envolver perguntas sobre a vida, perguntas sobre o gosto (em várias áreas), perguntas sobre história pessoal, etc. Adicionalmente, o número de perguntas deve ser grande o suficiente para criar a entropia desejada. Dependendo da implantação desejada, podem também ser empregados valores aleatórios que o usuário mantém no dispositivo portátil, ou em um pedaço de papel, ou é enviado por correio ao usuário e é mantido fora de contas de Internet: R1, R2, etc., e/ou valores aleatórios adicionais que o sistema local do usuário mantém e um S secreto.

[0054] O processamento pode envolver geração de fator. Considerando-se as entradas às perguntas: A1, A2,....An, as respostas são organizadas em grupos (com repetições), por exemplo, G1= A1, A3, A5, G2= A1, A3, A6, A7. Um grupo representa um conjunto de respostas concatenadas que se espera que o usuário responda de forma completa. Presumindo-se m grupos, em que cada grupo tem entropia alta o suficiente. Dependendo da implantação desejada, valores aleatórios R1,...Rm e o S secreto podem também ser adicionados (concatenados), por exemplo, S a cada grupo e Ri a Gi, de modo que G1= S, R1, A1, A3, A5.

[0055] Cada Gi é hasheado com uma função de hash criptográfico (por exemplo, Sha1, etc.) H. Por exemplo, H1= H(H(H(H(H(R), S1) A1)A3)A5). Hashing adicional para desacelerar a computação pode também ocorrer. Os H_is são chamados de indicadores.

[0056] Cada grupo tem seu próprio indicador Hi: H1, H2, ….Hm. Os valores Ri aleatórios, chamados de aleatorizadores, são mantidos no sistema de usuário (por exemplo, não acessíveis pelo servidor ou criptografados sob S e enviados ao servidor), e S é o segredo do usuário mantido fora do sistema (por exemplo, em um papel ou em outro dispositivo mantido para recuperação, ou em fiduciários, e em nenhum outro local). Seja E_S(Ri)=Xi, em que Xi é a criptografia de Ri usado em Hi e S é chamado de a semente. Hi, Xi i=1,..,m são enviados ao servidor. Os

indicadores His são, então, apagados no lado de cliente e em seu dispositivo.

[0057] S, a semente, é mantido na memória do usuário fora do armazenamento de conta (por exemplo, em um dispositivo ou um papel). Os His são enviados ao servidor para ser mantidos para a validação de recuperação, e a cópia local é apagada. O servidor pode realizar hash adicional nos indicadores com funções unidirecionais, para impedir que atacantes penetrantes aprendam os indicadores.

[0058] A partir da implantação exemplificativa acima, o servidor, portanto, recebe nenhuma informação sobre as respostas e somente recebe um valor hasheado com entropia suficiente. O usuário deve ter capacidade para responder perguntas suficientes para corresponder a um grupo. Um atacante não deve poder adivinhar as respostas para cobrir nem mesmo um grupo e não tem qualquer acesso ao S.

[0059] Os fatores podem, então, ser usados para a autorização. No processo de autenticação ou no processo de recuperação de conta, ocorre a tentativa de usar o fator persistente. O servidor apresenta as perguntas de um dentre os grupos, em que o usuário escolhe um grupo, responde às perguntas, insere seu S e seu dispositivo, por sua vez, recupera o Ri de Xi com o uso de seu S secreto. O Hi é computado do zero, com base nas respostas atuais do usuário, gerando o grupo de resposta Gi atual (um candidato para Gi) e o Hi gerado é enviado ao servidor. O usuário pode computar o indicador inteiro a partir das respostas; alternativamente, algumas das respostas nos indicadores (como A5 no exemplo) podem ser enviadas liberadas, e o indicador parcialmente avaliado H(H(H(H(R), S1) A1)A3) no exemplo pode ser enviado, e o usuário pode completar a computação do indicador (ou seja, algumas respostas são escondidas e algumas são abertas-- somente na recuperação).

[0060] O servidor compara o Hi gerado computado que é, então, hasheado com o Hi hasheado armazenado. Se houver uma correspondência, o usuário é autenticado. Caso contrário, o requerente (por exemplo, se o Hi gerado falhar em vários grupos) falha e não é reconhecido como o usuário original. Observe-se que, em uma implantação exemplificativa alternativa, o usuário pode se envolver em um protocolo que prove a posse de Hi, em relação a uma versão HASH(Hi) hasheada.

[0061] As respostas podem exigir informações pessoais sobre o usuário, mas as informações são todas locais ao computador de usuário ou o dispositivo de usuário e não são acessíveis por parte do servidor para fins de privacidade, tampouco são acessíveis a pessoas realizando phishing que finjam ser o servidor. Visto que as respostas são apagadas, são reconstruídas no momento de inquirição. Além disso, informações parciais podem ser fornecidas: tal como o hashing aninhado parcial é calculado, e o A5 é liberado, e o servidor conclui o hashing.

[0062] Para uma implantação tal como H(R)*H(A1)*H(A3)* H(A5) (isto é, uma multiplicação de hashes de valores individuais em um campo grande o suficiente) como a função de combinação, um produto parcial pode ser fornecido, em que algumas das respostas podem ser abertas, e o servidor pode completar o produto. Para um teste de posição fixa, H(R)*H(1, A1)*H(2, A3)* H(3, A5) pode ser fornecido, de modo que a resposta Ai na posição j do questionário seja associada à posição j. O produto pode ser realizado sobre um grande campo de ordem prima.

[0063] As informações devem ter entropia suficiente para esconder os campos individuais considerando-se o estado do servidor, de forma que a probabilidade de um atacante produzir a resposta seja substancialmente pequena. O usuário precisa, ainda, assegurar que o fator seja dado ao servidor correto. Tentar aprender o fator (ataques off-line) ou fatores que abrem algumas das respostas (ataques em tempo real) é possível e deve ser considerado na implantação.

[0064] Adicionalmente, ajudará nisso um conjunto de respostas altamente memorizadas ser usado, e o treinamento de usuário ser estabelecido antes de os valores serem comprometidos (gravados) no servidor. Respostas difíceis de lembrar podem ser anotadas, para se assegurar que o fator é persistente. As implantações exemplificativas podem ser de tal forma que um sistema de software geral possa ser empregado sem dispositivos/ leitores/ etc. especiais.

[0065] As implantações exemplificativas podem envolver um sistema ou processo em que as respostas sejam obtidas pelos usuários a partir de agências externas, em vez de lembradas. Essas agências confiam na autenticação para permitir que o usuário resgate a resposta, de modo que a implantação possa

construir uma “recuperação social” implícita com o uso do fator persistente acima. O fator pode ser construído de modo incremental, passando-se pelo teste anterior primeiro e, então, atualizando-se o conhecimento embutido no fator. Adicionalmente, o fator persistente pode ser restringido de modo que o mesmo seja usado quando necessário e pode ser sustentado por outros fatores e ser incluído como um fator decisivo adicional em um processo de recuperação de conta ou de retomada de conta. Observe-se que as respostas provenientes do usuário e de fiduciários podem ser obtidas empregando-se qualquer método de entrada: digitação, voz, leitura biométrica, câmera, etc.

[0066] As implantações exemplificativas descritas acima permitem, assim, que o usuário substitua uma senha com o conhecimento que o usuário insere. Diferentemente de senhas, o usuário muito provavelmente conhece diversos assuntos relacionados ao usuário (uma grande porção dos mesmos). O uso de senhas pode ser utilizado para descriptografia local de informações sobre senha criptografadas (como uma chave privada). Estender essa nova ideia pode ser usado para substituição temporária de senha para tais fins e é uma matéria de outro projeto em que o “dispositivo” é meramente computação local. A “computação local” pode ser realizada em um dispositivo móvel, e o resultado final, enviado ao computador ou servidor por meio de um método de comunicação local, tal como uma conexão sem fio, USB ou física, para assegurar ao usuário que as respostas não são roubadas.

[0067] As implantações exemplificativas podem também envolver um fator persistente que o usuário pode sempre reconstruir, mesmo se outros meios de identificação tiverem sido perdidos. Isso pode distinguir o usuário de um sequestrador de conta e ser usado para a retomada de contas por parte dos usuários (por exemplo, um método de retomada com base em questionário e na minimização de exposição é estabelecido).

[0068] A Figura 1(a) ilustra um fluxograma para um dispositivo, de acordo com uma implantação exemplificativa. Em 100, o dispositivo gera uma pluralidade de hashes provenientes de uma pluralidade de respostas fornecidas pelo usuário, a

uma pluralidade de perguntas. As perguntas fornecidas podem ser provenientes de um servidor, ou do dispositivo, e utilizarem um questionário que envolve informações pessoais sobre o usuário conforme descrito acima.

[0069] Em 101, o dispositivo pode gerar um hash de autenticação a partir da pluralidade de hashes. Isso pode ser implantado executando-se uma interpolação polinomial da pluralidade de hashes para gerar o hash de autenticação, e/ou selecionando-se um ou mais dentre a pluralidade de hashes para formar o hash de autenticação com base em um grupo selecionado dentre a pluralidade de perguntas. Conforme descrito nas implantações exemplificativas acima, o usuário pode selecionar um grupo de perguntas para responder, e as respostas podem, assim, ser hasheadas para gerar o hash de autenticação, ou o dispositivo pode selecionar um subconjunto das respostas fornecidas (por exemplo, duas ou mais) e gerar um hash de autenticação com base no subconjunto. Conforme descrito nas implantações exemplificativas acima, um hash de autenticação secreto pode também ser armazenado no dispositivo e encaminhado ao servidor por um protocolo seguro quando os requisitos forem atendidos (por exemplo, atender a um limite de respostas corretas às perguntas, responder um subconjunto das perguntas corretamente, o hash de autenticação corresponder ao hash de autenticação secreto, etc.).

[0070] O dispositivo pode também gerar o hash de autenticação a partir de uma interpolação polinomial da pluralidade de hashes a partir do uso de uma interpolação polinomial para interpolar o hash de autenticação, conforme descrito acima. Implantações tais como o algoritmo de interpolação polinomial e o algoritmo de interpolação ruidosa podem ser empregadas. Um limite pode ser ajustado e aplicado à interpolação polinomial através da introdução de um ou mais pontos errôneos para a interpolação polinomial, com o uso de pontos adicionais no servidor e/ou um ou mais pontos corretos para a interpolação polinomial. Em 102, o dispositivo, então, tenta autenticar no servidor com o hash de autenticação gerado.

[0071] A Figura 1(b) ilustra um fluxograma para um processo de recuperação, de acordo com uma implantação exemplificativa. Conforme descrito nas implantações

exemplificativas acima, em 103, o dispositivo recebe uma pluralidade de perguntas, dentre as quais o usuário pode selecionar um subconjunto para responder para recuperar o acesso à conta. Em 104, as respostas fornecidas são convertidas em um hash de autenticação com base no uso de um número aleatório gerado a partir de uma semente secreta que está fora do dispositivo de usuário. Em 105, o hash de autenticação é encaminhado ao servidor.

[0072] A Figura 2(a) ilustra um fluxograma para um servidor, de acordo com uma implantação exemplificativa. Em 200, o servidor pode transmitir uma pluralidade de perguntas pessoais ao dispositivo. Em 201, o servidor recebe um hash de autenticação a partir de um dispositivo em resposta à pluralidade de perguntas transmitidas. Em 202, o servidor pode, então, decidir conceder acesso 204 (SIM) quando um hash de autenticação responsivo à pluralidade de perguntas transmitidas corresponder a um hash de autenticação secreto armazenado no servidor; e negar acesso 203 (NÃO) quando o hash de autenticação não corresponder ao hash de autenticação secreto. O hash de autenticação pode ser gerado a partir de uma interpolação polinomial da pluralidade de hashes e de uma seleção de um ou mais dentre a pluralidade de hashes para formar o hash de autenticação com base em um grupo selecionado dentre a pluralidade de perguntas. Dependendo da implantação, o servidor pode transmitir um ou mais pontos errôneos e um ou mais pontos corretos para uso em um algoritmo de interpolação ruidosa, com base no hash de autenticação secreto e em um limite. O servidor pode também realizar hashing do hash de autenticação recebido para determinar se o hash corresponde ao hash secreto armazenado.

[0073] Em outro exemplo, o servidor pode selecionar o hash de autenticação secreto a partir de uma pluralidade de hashes de autenticação secretos com base em um grupo selecionado das perguntas transmitidas, em que cada um dentre a pluralidade de hashes de autenticação secretos é associado a pelo menos duas dentre a pluralidade de perguntas. O grupo selecionado de perguntas transmitidas pode ser selecionado no dispositivo ou pelo servidor. Isso pode ser implantado, por exemplo, em um processo de recuperação conforme descrito acima.

[0074] A Figura 2(b) ilustra um fluxograma para um processo de recuperação a partir do servidor, de acordo com uma implantação exemplificativa. Em 205, o servidor pode transmitir uma pluralidade de perguntas pessoais ao dispositivo. Em 206, o servidor recebe um hash de autenticação proveniente de um dispositivo em resposta à pluralidade de perguntas transmitidas, em que o hash de autenticação é potencialmente um dentre os indicadores conforme descrito nas implantações exemplificativas acima. Em 207, o servidor pode, então, decidir iniciar um processo para recuperar a conta de usuário 209 (SIM) quando o hash de autenticação corresponder a um dentre os indicadores armazenados no servidor; e negar acesso 208 (NÃO) quando o hash de autenticação não corresponder a qualquer dentre os indicadores armazenados.

AMBIENTE DE PROCESSAMENTO EXEMPLIFICATIVO

[0075] A Figura 3 mostra um ambiente de computação exemplificativo com um dispositivo de computação exemplificativo adequado para uso em algumas implantações exemplificativas. O dispositivo de computação 305 no ambiente de computação 300 pode incluir uma ou mais unidades de processamento, núcleos, ou processadores 310, memória 315 (por exemplo, RAM, ROM e/ou similares), armazenamento interno 320 (por exemplo, magnético, óptico, armazenamento de estado sólido e/ou orgânico), e/ou interface de I/O 325, qualquer um dentre os quais pode ser acoplado em um mecanismo de comunicação ou um barramento 330 para comunicar informações ou embutido no dispositivo de computação 305.

[0076] O dispositivo de computação 305 pode ser acoplado de modo comunicativo à entrada/interface de usuário 325 e ao dispositivo de saída/à interface 340. Tanto um quanto ambos dentre entrada/interface de usuário 325 e dispositivo de saída/interface 340 podem ser uma interface com ou sem fio e podem ser removíveis. Entrada/interface de usuário 325 podem incluir qualquer dispositivo, componente, sensor ou interface, físico ou virtual, que podem ser usados para fornecer entrada (por exemplo, botões, interface de tela sensível ao toque, teclado, um controle de apontamento/cursor, microfone, câmera, braille, sensor de movimento, leitor óptico e/ou similares). O dispositivo de saída/a interface 340

podem incluir um visor, uma televisão, um monitor, uma impressora, um alto-falante, um braille ou similares. Em algumas implantações exemplificativas, a entrada/interface de usuário 325 e o dispositivo de saída/a interface 340 podem ser embutidos ou acoplados fisicamente ao dispositivo de computação 305. Em outras implantações exemplificativas, outros dispositivos de computação podem funcionar como ou fornecer as funções de entrada/interface de usuário 325 e dispositivo de saída/interface 340 para um dispositivo de computação 605.

[0077] Exemplos de dispositivo de computação 305 podem incluir, porém, sem limitação, dispositivos altamente móveis (por exemplo, dispositivos tipo smartphone, dispositivos em veículos e outras máquinas, dispositivos portados por seres humanos e animais e similares), dispositivos móveis (por exemplo, dispositivos tipo tablet, dispositivos tipo notebook, dispositivos tipo laptop, computadores pessoais, televisões portáteis, rádios e similares) e dispositivos não projetados para mobilidade (por exemplo, computadores de mesa, outros computadores, quiosques de informações, televisões com um ou mais processadores embutidos nas mesmas e/ou acoplados às mesmas, rádios, servidores e similares).

[0078] O dispositivo de computação 305 pode ser acoplado de modo comunicativo (por exemplo, por meio de interface de I/O 325) ao armazenamento externo 345 e à rede 350 para se comunicar com qualquer quantidade de componentes, dispositivos e sistemas de rede, incluindo um ou mais dispositivos de computação com configuração igual ou diferente. O dispositivo de computação 305 ou qualquer dispositivo de computação conectado pode funcionar como, fornecer serviços de ou ser referido como um servidor, um cliente, um servidor fino, uma máquina geral, uma máquina de finalidade especial ou outra identificação.

[0079] A interface de I/O 325 pode incluir, porém, sem limitação, interfaces com e/ou sem fio com o uso de quaisquer protocolos ou padrões de comunicação ou I/O (por exemplo, Ethernet, 802.11x, Universal System Bus, WiMax, modem, um protocolo de rede de celular e similares) para comunicar informações a e/ou a partir de pelo menos todos os componentes conectados, dispositivos e rede no ambiente de computação 300. A rede 350 pode ser qualquer rede ou combinação de redes

(por exemplo, a Internet, uma rede de área local, uma rede de área ampla, uma rede telefônica, uma rede de celular, uma rede de satélite e similares).

[0080] O dispositivo de computação 305 pode usar e/ou se comunicar com o uso de mídia usável ou legível por computador, incluindo mídia de sinal e mídia de armazenamento. Mídia de sinal inclui mídia de transmissão (por exemplo, cabos metálicos, fibra óptica), sinais, ondas portadoras e similares. Mídia de armazenamento inclui mídia magnética (por exemplo, discos e fitas), mídia óptica (por exemplo, CD ROM, discos de vídeo digital, discos de Blu-ray), mídia de estado sólido (por exemplo, RAM, ROM, memória flash, armazenamento de estado sólido) e outro armazenamento ou outra memória não volátil.

[0081] O dispositivo de computação 305 pode ser usado para implantar técnicas, métodos, aplicativos, processos ou instruções executáveis por computador em alguns ambientes de computação exemplificativos. As instruções executáveis por computador podem ser resgatadas a partir de mídia transitória e armazenadas em mídia não transitória ou resgatadas da mesma. As instruções executáveis podem se originar a partir de um ou mais dentre quaisquer linguagens de programação, de scripts e de máquinas (por exemplo, C, C++, C#, Java, Visual Basic, Python, Perl, JavaScript e outras).

[0082] O(s) processador(es) 310 pode(m) ser executado(s) sob qualquer sistema operacional (OS) (não mostrado), em um ambiente nativo ou virtual. Podem ser empregados um ou mais aplicativos que incluam unidade lógica 360, unidade de interface de programação de aplicativo (API) 365, unidade de entrada 370, unidade de saída 375, unidade de autenticação 380, unidade de recuperação 385, unidade geradora de número aleatório 390 e mecanismo de comunicação entre unidades 395 para as diferentes unidades se comunicarem umas com as outras, com o OS e com outros aplicativos (não mostrado). Por exemplo, a unidade de autenticação 380, a unidade de recuperação 385 e a unidade geradora de número aleatório 390 podem implantar um ou mais processos conforme mostrado nas Figuras 1(a), 1(b), 2(a) e 2(b), dependendo da implantação como um dispositivo ou um servidor. A unidade de recuperação 385 pode também implantar os processos de recuperação conforme

descrito nas implantações exemplificativas acima das Figuras 1(b) e 2(b). As unidades e os elementos descritos podem variar em projeto, função, configuração ou implantação e não são limitados às descrições fornecidas.

[0083] Em algumas implantações exemplificativas, quando informações ou uma instrução de execução são recebidas pela unidade de API 365, as mesmas podem ser comunicadas a uma ou mais outras unidades (por exemplo, unidade lógica 360, unidade de entrada 370, unidade de saída 375, unidade de autenticação 380, unidade de recuperação 385 e unidade geradora de número aleatório 390). Por exemplo, a unidade geradora de número aleatório 390 pode ser usada para gerar hashes ou selecionar perguntas para submissão e usar a unidade de API 365 para se comunicar com a unidade de autenticação 380 e a unidade de recuperação 385 para fornecer números aleatórios conforme descrito nas implantações exemplificativas acima. A unidade de autenticação 380 pode, por meio da unidade de API 365, interagir com a unidade de recuperação 385 para comparar um hash de autenticação com um hash de autenticação secreto armazenado.

[0084] Em alguns casos, a unidade lógica 360 pode ser configurada para controlar o fluxo de informações entre as unidades e direcionar os serviços fornecidos pela unidade de API 365, pela unidade de entrada 370, pela unidade de saída 375, pela unidade de autenticação 380, pela unidade de recuperação 385 e pela unidade geradora de número aleatório 390 em algumas implantações exemplificativas descritas acima. Por exemplo, o fluxo de um ou mais processos ou implantações pode ser controlado pela unidade lógica 360 sozinha ou em conjunto com a unidade de API 365.

AMBIENTE DE PROCESSAMENTO EXEMPLIFICATIVO

[0085] A Figura 4 mostra um ambiente online exemplificativo em que algumas modalidades exemplificativas podem ser implantadas. O ambiente 400 inclui os dispositivos 405 a 445, em que cada um é conectado de modo comunicativo a pelo menos um outro dispositivo por meio, por exemplo, da rede 450. Alguns dispositivos podem ser conectados de modo comunicativo a um ou mais dispositivos de armazenamento 430 e 445 (por exemplo, por meio do dispositivo 425).

[0086] Um exemplo de um ou mais dispositivos 405 a 450 pode ser o dispositivo de computação 605 descrito abaixo na Figura 6. Os dispositivos 405 a 450 podem incluir, porém, sem limitação, um computador 425 (por exemplo, pessoal ou comercial), um dispositivo associado a um veículo 420, um dispositivo móvel 410 (por exemplo, um dispositivo tipo smartphone), uma televisão 415, um computador móvel 405, um computador de servidor 450, dispositivos de computação 435 a 440, dispositivos de armazenamento 430, 445. Qualquer um dentre os dispositivos 405 a 450 podem acessar um ou mais serviços a partir de e/ou fornecer um ou mais serviços a um ou mais dispositivos mostrados no ambiente 400 e/ou dispositivos não mostrados no ambiente 400. O acesso entre os dispositivos pode ser com fio, sem fio e por meio de comunicação multimídia como voz de usuário, fotos de câmera, etc.

[0087] Um usuário pode controlar um dispositivo, conforme explicado acima, para implantar as implantações exemplificativas, por meio da rede 450. As informações associadas às implantações exemplificativas podem ser armazenadas no dispositivo de armazenamento 430 ou 445, respectivamente, por exemplo.

[0088] Em situações em que os sistemas discutidos aqui coletem informações pessoais sobre os usuários ou possam fazer uso de informações pessoais, os usuários podem ter a oportunidade de controlar se os programas ou recursos coletarão informações de usuário (por exemplo, informações sobre a rede social de um usuário, ações sociais ou atividades, profissão, as preferências de um usuário ou a localização atual de um usuário) ou de controlar se e/ou como receber conteúdo a partir do servidor de conteúdo que pode ser mais relevante ao usuário. Além disso, certos dados podem ser tratados de uma ou mais formas antes de serem armazenados ou usados, de modo que informações pessoalmente identificáveis sejam removidas. Por exemplo, a identidade de um usuário pode ser tratada de modo que nenhuma informação pessoalmente identificável possa ser determinada para o usuário, ou a localização geográfica de um usuário pode ser generalizada onde as informações de localização são obtidas (tal como a nível de uma cidade, de um CEP ou de um estado), de modo que uma localização particular de um usuário

não possa ser determinada. Assim, o usuário pode ter controle sobre como as informações sobre o usuário são coletadas e usadas por um servidor de conteúdo.

[0089] Embora algumas implantações exemplificativas tenham sido mostradas e descritas, essas implantações exemplificativas são fornecidas para transmitir a matéria descrita no presente documento a pessoas que estão familiarizadas com esse campo. Deve-se entender que a matéria descrita no presente documento pode ser implantada de várias formas sem ser limitada às implantações exemplificativas descritas. A matéria descrita no presente documento pode ser praticada sem essas matérias especificamente definidas ou descritas ou com outros ou diferentes elementos ou matérias não descritos. Será compreendido por aqueles familiarizados com esse campo que mudanças podem ser feitas nessas implantações exemplificativas sem se afastar da matéria descrita no presente documento conforme definido nas reivindicações anexas e seus equivalentes.

REIVINDICAÇÕES

1. Dispositivo, caracterizado pelo fato de que compreende:

um processador, configurado para:

gerar uma pluralidade de hashes a partir de uma pluralidade de respostas a uma pluralidade de perguntas;

gerar um hash de autenticação a partir de uma interpolação polinomial da pluralidade de hashes e operações algébricas sobre a pluralidade de hashes através do uso de um algoritmo de interpolação ruidosa, e ajustar um limite do algoritmo de interpolação ruidosa através da introdução de um dentre: um ou mais pontos errôneos para a interpolação polinomial e um ou mais pontos para a interpolação polinomial; e

autenticar com o hash de autenticação, e

uma memória configurada para armazenar o hash de autenticação.

2. Dispositivo, de acordo com a reivindicação 1, caracterizado pelo fato de que o processador é configurado para gerar o hash de autenticação a partir da seleção com base em uma seleção de um dentre a pluralidade de hashes como o hash de autenticação, e em que o processador é configurado para gerar cada um dentre a pluralidade de hashes a partir de pelo menos duas dentre a pluralidade de respostas.

3. Dispositivo, de acordo com a reivindicação 1, caracterizado pelo fato de que compreende adicionalmente uma memória configurada para armazenar um hash de autenticação secreto, e em que o processador é configurado para autenticar com o hash de autenticação através de uma comparação do hash de autenticação secreto com o hash de autenticação, e configurado adicionalmente para:

usar o hash de autenticação secreto para autenticação quando o hash de autenticação corresponder ao hash de autenticação secreto, e

negar a autenticação quando o hash de autenticação não corresponder ao hash de autenticação secreto.

4. Dispositivo, de acordo com a reivindicação 1, caracterizado pelo fato de que o processador é configurado para gerar o hash de autenticação a partir da seleção com base no uso da pluralidade de hashes que corresponde à pluralidade de respostas associada ao grupo selecionado dentre a pluralidade de perguntas para formar o hash de autenticação.

5. Mídia de armazenamento legível por computador, caracterizada pelo fato de que armazena instruções para executar um processo, sendo que as instruções compreendem:

gerar uma pluralidade de hashes a partir de uma pluralidade respostas a uma pluralidade de perguntas;

gerar uma hash de autenticação a partir de uma interpolação polinomial da pluralidade de hashes e operações algébricas sobre a pluralidade de hashes através do uso de um algoritmo de interpolação ruidosa, e ajustar um limite do algoritmo de interpolação ruidosa através da introdução de um dentre: um ou mais pontos errôneos para a interpolação polinomial e um ou mais pontos para a interpolação polinomial; e

autenticar com o hash de autenticação.

6. Mídia de armazenamento legível por computador, de acordo com a reivindicação 5, caracterizada pelo fato de que a geração do hash de autenticação a partir da pluralidade de hashes compreende realizar uma interpolação polinomial da pluralidade de hashes.

7. Mídia de armazenamento legível por computador, de acordo com a reivindicação 6, caracterizada pelo fato de que a autenticação com o hash de autenticação compreende:

comparar um hash de autenticação secreto com o hash de autenticação;

usar o hash de autenticação secreto para autenticação quando o hash de autenticação corresponder ao hash de autenticação secreto, e

negar a autenticação quando o hash de autenticação não corresponder ao hash de autenticação secreto.

8. Mídia de armazenamento legível por computador, de acordo com a reivindicação 5, caracterizada pelo fato de que cada um dentre a pluralidade de hashes é gerado a partir de pelo menos duas dentre a pluralidade de respostas; e em que gerar o hash de autenticação a partir da pluralidade de hashes compreende selecionar um dentre a pluralidade de hashes como o hash de autenticação com base em um grupo selecionado dentre a pluralidade de perguntas.

9. Servidor caracterizado pelo fato de que compreende:

um processador configurado para:

transmitir uma pluralidade de perguntas; e

conceder acesso quando um hash de autenticação responsivo à pluralidade de perguntas transmitidas corresponder a um hash de autenticação secreto; e

negar acesso quando o hash de autenticação não corresponder ao hash de autenticação secreto;

em que o hash de autenticação é gerado a partir de uma interpolação polinomial da pluralidade de hashes e operações algébricas sobre a pluralidade de hashes através do uso de um algoritmo de interpolação ruidosa, e ajustar um limite do algoritmo de interpolação ruidosa através da introdução de um dentre: um ou mais pontos errôneos para a interpolação polinomial e um ou mais pontos para a interpolação polinomial; e

uma memória configurada para armazenar o hash de autenticação.

10. Servidor, de acordo com a reivindicação 9, caracterizado pelo fato de que o processador é configurado para gerar e transmitir pelo menos um dentre: um ou mais pontos errôneos e um ou mais pontos corretos para uso em um algoritmo de interpolação ruidosa, com base no hash de autenticação secreto e em um limite.

11. Servidor, de acordo com a reivindicação 9, caracterizado pelo fato de que o processador é configurado para selecionar o hash de autenticação secreto a partir de uma pluralidade de hashes de autenticação secretos com base em um grupo selecionado das perguntas transmitidas, em que cada um dentre a pluralidade de hashes de autenticação secretos é associado a pelo menos duas dentre a pluralidade de perguntas.

12. Servidor, de acordo com a reivindicação 9, caracterizado pelo fato de que o processador é configurado adicionalmente para:

receber uma resposta à pluralidade de perguntas, sendo que a resposta compreende um hash de resposta e uma resposta a uma ou um subconjunto da pluralidade de perguntas; e

construir o hash de autenticação a partir do hash de resposta e da pergunta.

13. Servidor, de acordo com a reivindicação 12, caracterizado pelo fato de que o processador é configurado para construir o hash de autenticação pela construção de um hash aninhado a partir do hash de resposta e da resposta.

14. Servidor, de acordo com a reivindicação 12, caracterizado pelo fato de que o processador é configurado para construir o hash de autenticação pela multiplicação do hash de resposta por um hash da resposta.

15. Servidor, de acordo com a reivindicação 9, caracterizado pelo fato de que o processador é configurado adicionalmente para receber o hash de autenticação secreto e armazenar o hash de autenticação secreto em uma memória após receber uma confirmação a partir de um dispositivo associado a um usuário e uma conta associada ao usuário.

16. Servidor, de acordo com a reivindicação 9, caracterizado pelo fato de que a pluralidade de perguntas compreende uma solicitação por informações biométricas.

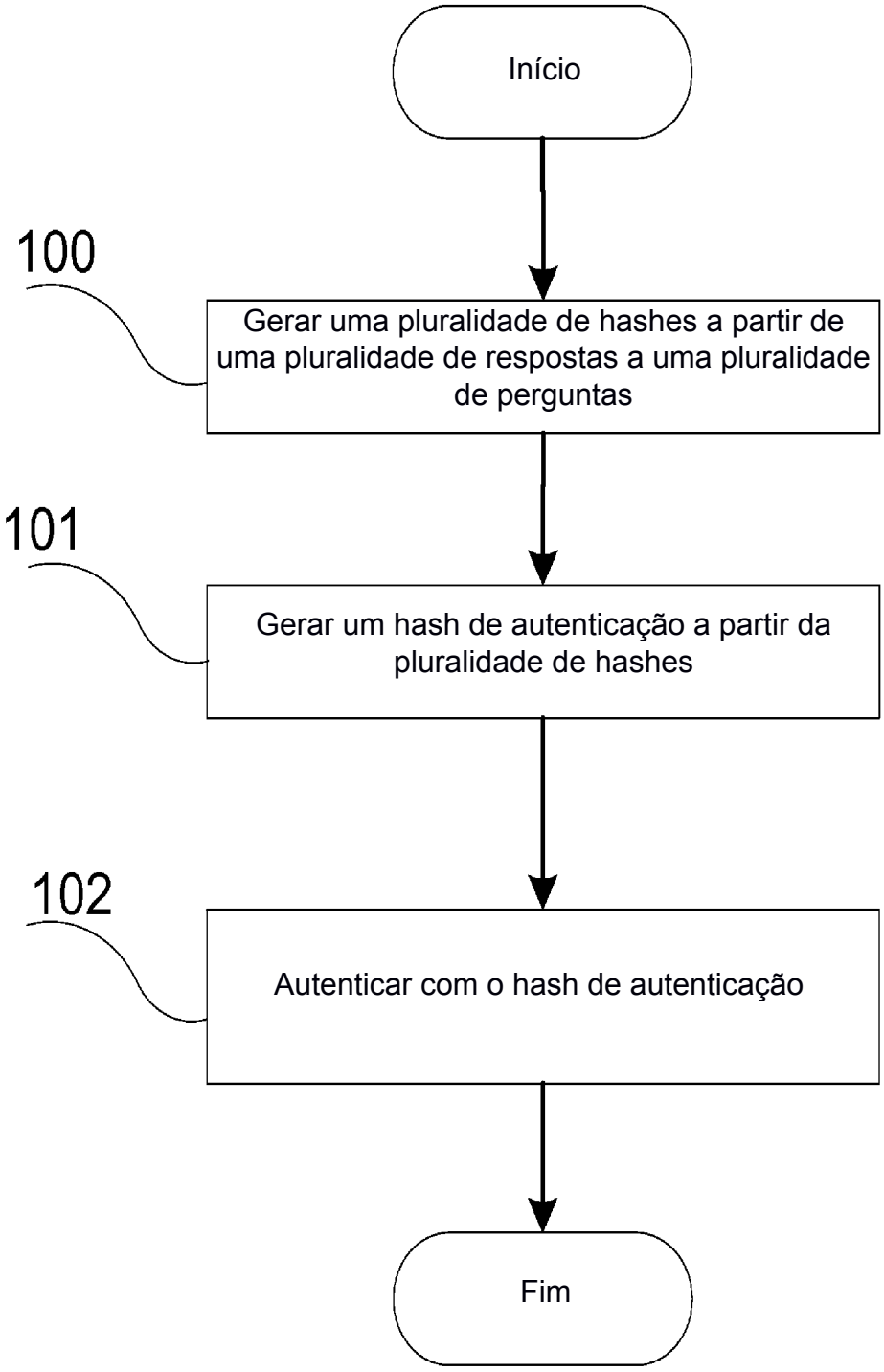
Início
100
Gerar uma pluralidade de hashes a partir de uma pluralidade de respostas a uma pluralidade de perguntas
101
Gerar um hash de autenticação a partir da pluralidade de hashes
102
Autenticar com o hash de autenticação
Fim

FIG. 1(a)

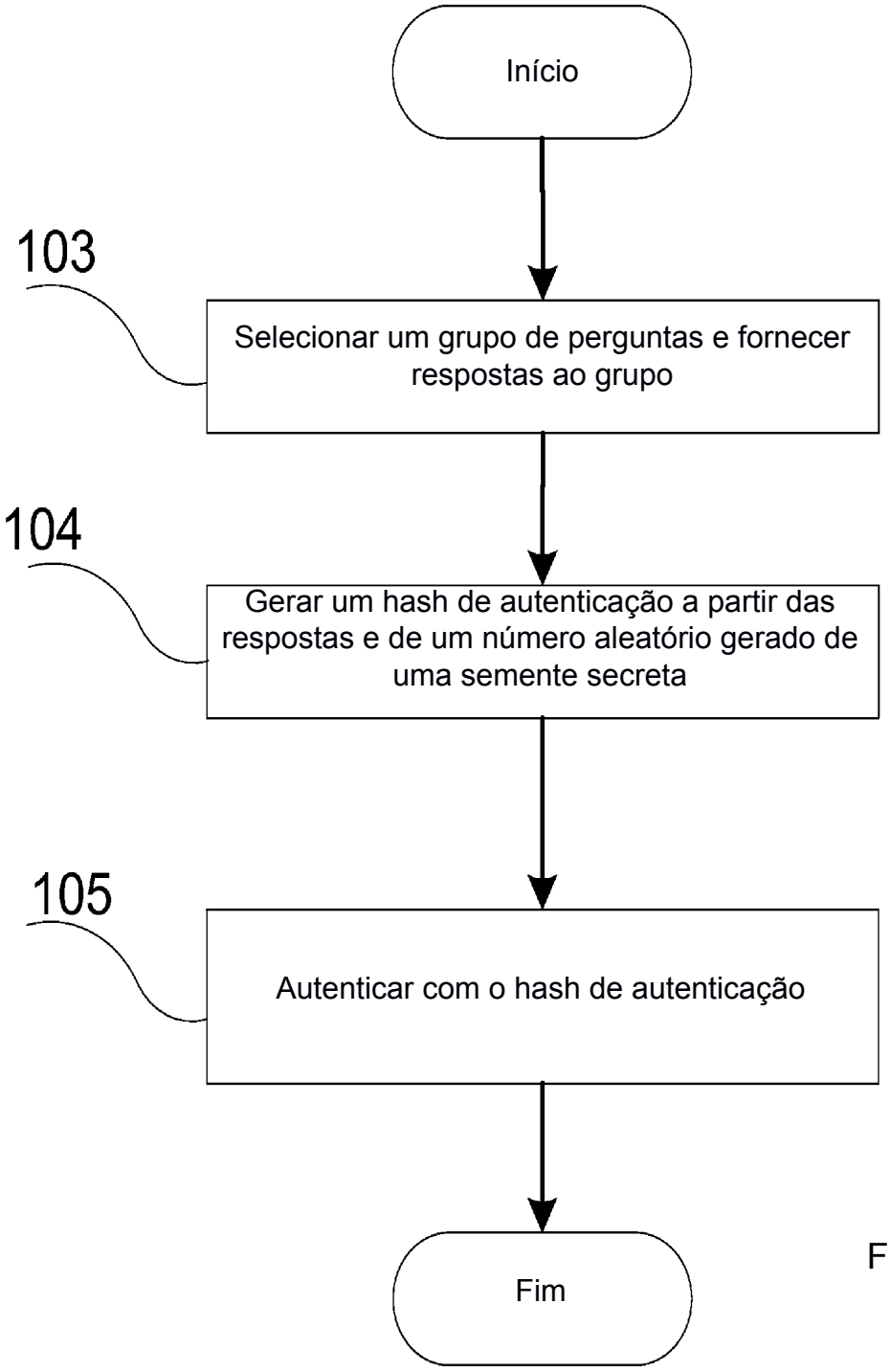
Início
103
Selecionar um grupo de perguntas e fornecer respostas ao grupo
104
Gerar um hash de autenticação a partir das respostas e de um número aleatório gerado de uma semente secreta
105
Autenticar com o hash de autenticação
Fim

FIG. 1(b)

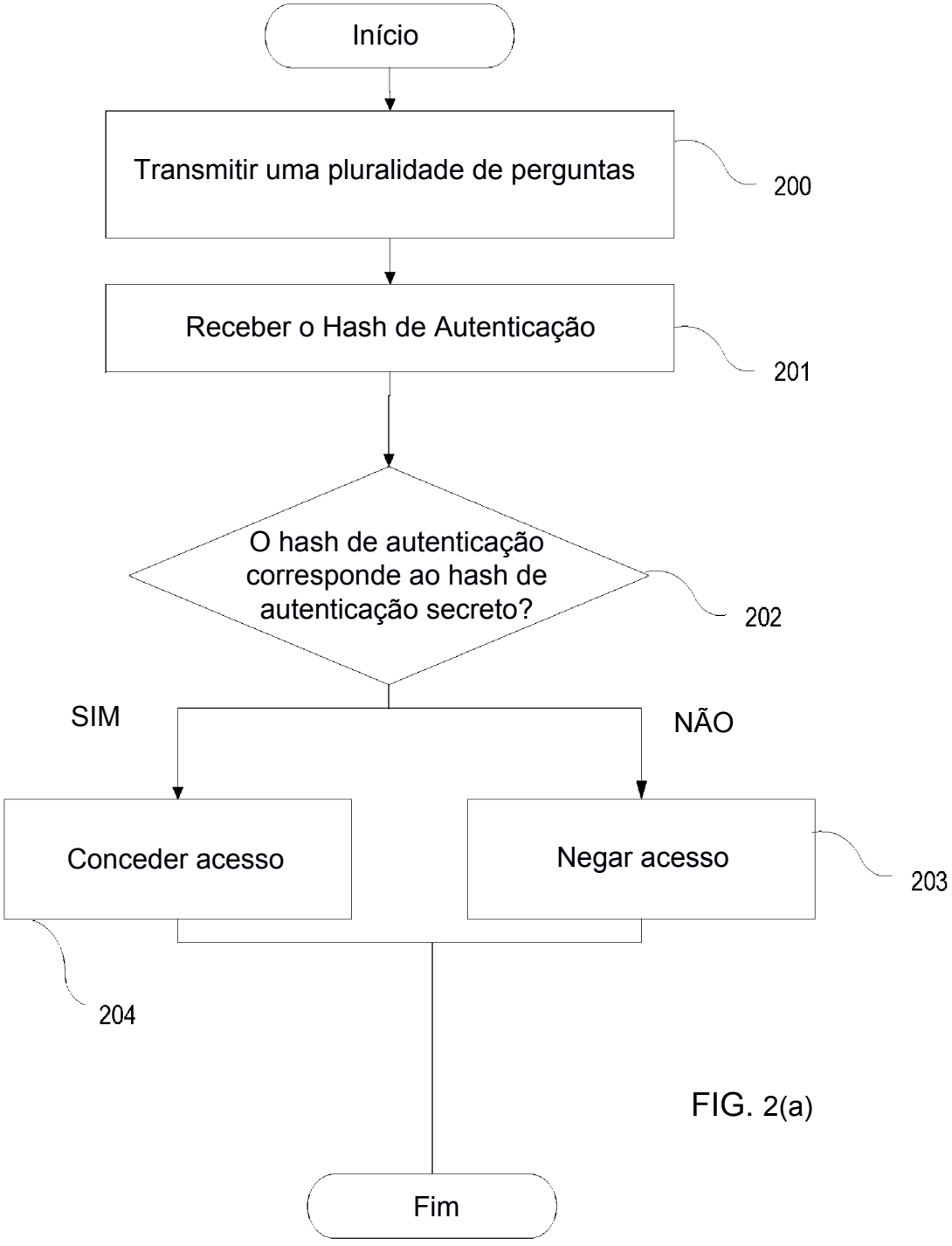
Início
Transmitir uma pluralidade de perguntas
200
Receber o Hash de Autenticação
201
O hash de autenticação corresponde ao hash de autenticação secreto?
202
SIM
NÃO
Conceder acesso
Negar acesso
203
204
Fim

FIG. 2(a)

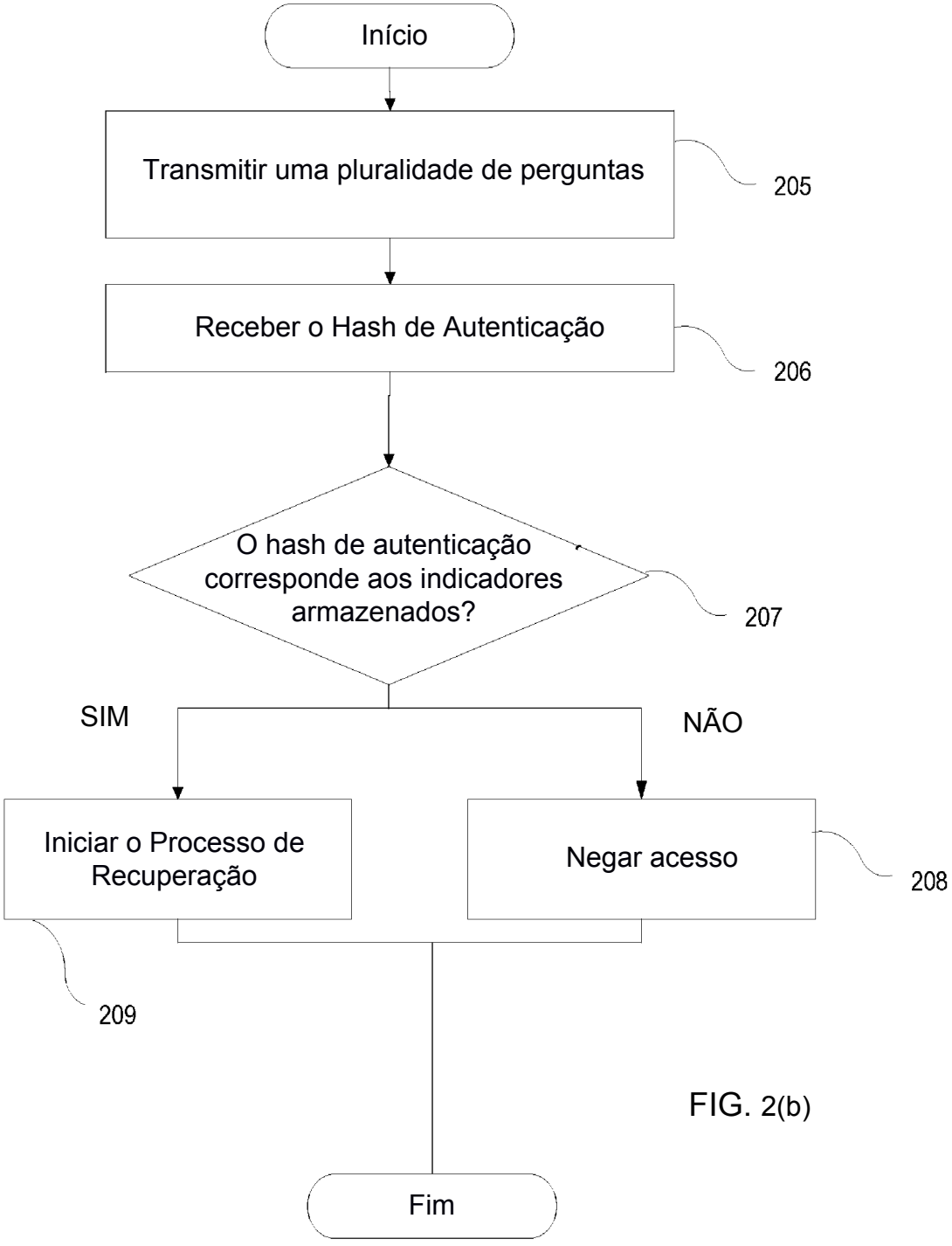
Início
Transmitir uma pluralidade de perguntas
205
Receber o Hash de Autenticação
206
O hash de autenticação corresponde aos indicadores armazenados?
207
SIM
NÃO
Iniciar o Processo de Recuperação
Negar acesso
208
209
Fim

FIG. 2(b)

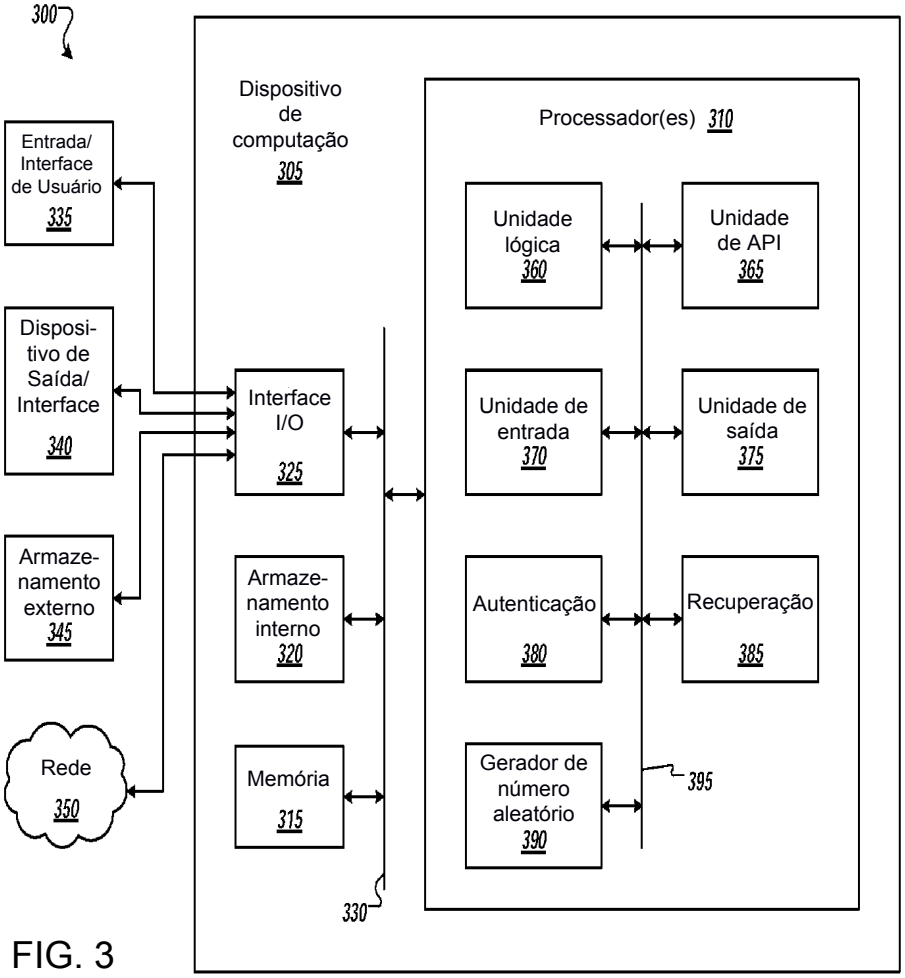
300
Dispositivo de computação 305
Processador(es) 310
Entrada/ Interface de Usuário 335
Dispositivo de Saída/ Interface 340
Armazenamento externo 345
Rede 350
Interface I/O 325
Armazenamento interno 320
Memória 315
330
Unidade lógica 360
Unidade de API 365
Unidade de entrada 370
Unidade de saída 375
Autenticação 380
Recuperação 385
Gerador de número aleatório 390
395

FIG. 3

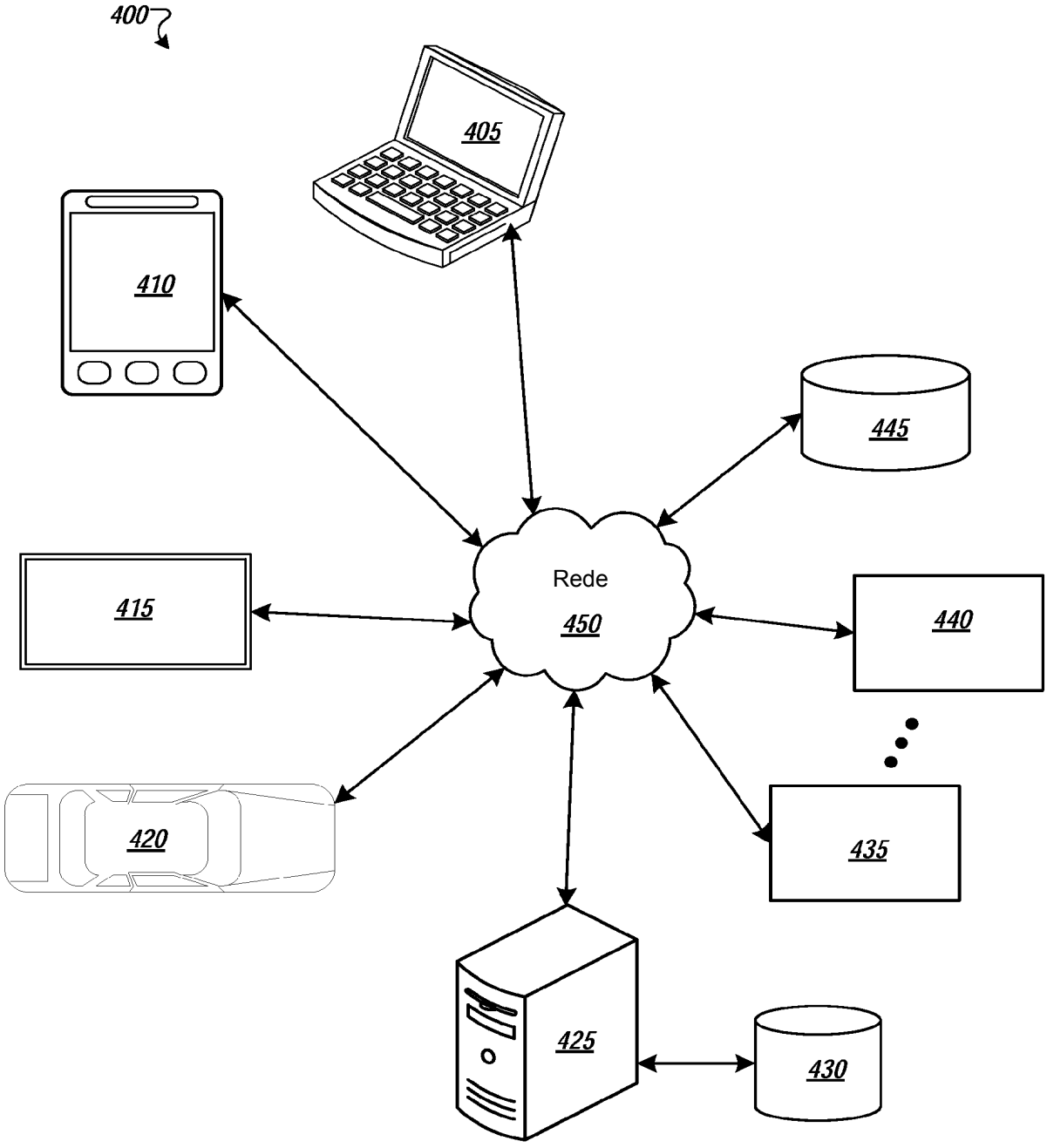

FIG. 4