Junho de 2014

Você Escolheu um Provedor de Identidade recentemente?

Robin Wilton
Diretor de Divulgação Técnica, Identidade e Privacidade

Internet Society

Resumo

Neste artigo técnico iremos analisar o mundo em constante mudança da gestão de identidade. A identidade digital está evoluindo a partir de um modelo de "retrospectiva" para um outro modelo altamente previsível, com base tanto em dados comportamentais, como nas tradicionais credenciais. Há também uma mudança a partir de credenciais fragmentadas para asserções de identidades e atributos mais transmissíveis. Potencialmente, essas mudanças oferecem uma maior escolha e poder ao indivíduo, mas apenas em potencial. Os modelos de identidade emergentes também contêm armadilhas escondidas, sobre as quais os usuários precisam estar cientes, para influenciarem o mercado através de exercícios de escolha efetivos.

Contexto

O mundo da identidade digital continua a evoluir a bom ritmo. O conceito de identidade digital em si, engloba várias formas diferentes, principalmente as três seguintes:

- identidades tradicionais "retrospectivas", onde se passa por um processo de atribuição de confiança para receber, a partir de terceiros, uma credencial que poderá mais tarde apresentar para se autenticar a si mesmo;
- identidades de baixa confiança "auto-confirmadas", onde um terceiro faz pouco mais do que lhe atribuir um documento de identificação sintaticamente correto, que será confirmado quando pedido;
- identidades "comportamentais", onde os prestadores de serviços recolhem dados suficientes sobre um indivíduo para dizer que a mesma pessoa irá visitar várias vezes.

É importante notar que o terceiro tipo de identificação (comportamental) poderá não exigir nenhuma ação explícita por parte do usuário. Se um site define um cookie do navegador, ou anota o seu endereço de IP, isso é suficiente para formar a base de uma identidade comportamental - embora existam também maneiras muito mais sofisticadas.

Os fornecedores de identidade (IDP) também evoluíram, e continuam a fazê-lo. O primeiro IDP que a maioria dos usuários encontra é provavelmente um destes três tipos:

- o governo (especialmente em caso de credenciais não-digitais como passaportes, carteira de motorista e assim por diante);
- um estabelecimento de ensino (a emissão de um cartão de estudante para acesso online aos recursos de estudante, bibliotecas, redes etc);
- um empregador (a emissão de informações de login do e-mail, aplicações de negócios, dentre outros exemplos).

Para simplificar um pouco: todos estes IDP emitem credenciais fragmentadas. Uma credencial emitida pelo governo provavelmente não poderá ser utilizada para iniciar a sessão nos sistemas do empregador (a menos que eles sejam a mesma coisa, o que obviamente é um caso especial). O cartão de estudante que usou durante toda a universidade, provavelmente não irá funcionar para os sistemas do seu empregador. Como referido, esta é uma simplificação - esquemas de identidade federados que

permitem que a distância entre os fragmentos sejam aproximadas; mas é mais comum as federações limitarem o seu alcance para, digamos, o contexto do ensino superior, ou o contexto do governo, ou simplesmente autenticações em organizações comerciais1.

Opção

Outra característica notável sobre todos estes três exemplos é que, enquanto usuário, você tem muito pouca ou nenhuma escolha no assunto. Ao se inscrever numa universidade ou aceitar um emprego, provavelmente não terá nenhuma opção a não ser inscrever-se no serviço de autenticação oferecido, ou enfrentar a probabilidade de tentar trabalhar sem acesso a recursos online (o que nos dias de hoje é muitas vezes impossível).

Existem duas maneiras para que a escolha entre nesta equação. Primeiro, com o surgimento de esquemas como o OpenID e o OAuth, os usuários ganharam a opção de auto-confirmar a sua guarda de um recurso (como um endereço de e-mail ou uma conta online), e, assim, por implicação, a sua identidade.

Em segundo lugar, esquemas como o Thawte da "Web of Trust" (agora infelizmente interrompido) ou o emergente UnitedID[2], procuram oferecer aos usuários uma credencial persistente associada a um identificador auto-confirmado (como um endereço de e-mail ou um token de autenticação). O UnitedID é particularmente interessante, na medida em que visa proporcionar uma identidade online de confiança para o consumidor do mercado de massas, sem ter que recorrer ao modelo de prestação de serviços online comum e comercial financiado por publicidade.

Essa credencial pode ou não ser inerentemente confiável. Depende, inicialmente, de quão confiável é o processo de inscrição. Se for muito fácil para obter uma credencial sintaticamente válida que diz que eu sou a Grace Kelly, a utilidade do sistema é comprometida. No entanto, se a credencial for suficientemente persistente, poderá não ser importante se parece dizer que sou a Grace Kelly: ao longo do tempo, um identificador persistente pode "agregar" confiabilidade exatamente da mesma maneira que um ser humano o faz, ou seja, através da construção de um registo de comportamento consistentemente confiável.

Mas espere: não existe outra categoria de IDP que oferece aos usuários uma escolha e permite que se autentiquem em vários prestadores de serviços diferentes? De certa forma, sim. Se alguma vez aceitou a oferta para iniciar uma sessão em um determinado serviço "X", usando a sua ID do Google, Facebook ou Twitter (para citar algumas das opções habituais), então "adquiriu" um IDP por predefinição, sem nunca ter conscientemente escolhido um. De certa forma, poderá ser mais exato dizer que optou por usar um IDP que foi pré-selecionado para si. Por enquanto, refiro-me a estes como "IDP sociais". Há implicações de privacidade que devem ser consideradas cuidadosamente...

---

[1] Existem exceções notáveis, como o sistema escandinavo BankID, que atravessa o fosso do sector comercial / público, e federações na indústria de defesa / aeroespacial, onde existe um alto grau de interação entre as agências governamentais e os seus contratantes.

[2] Página inicial da United ID: http://unitedid.org/about/

Implicações

Uma das opções que eu mencionei acima foi a opção de auto-confirmação (OpenID, OAuth, UnitedID e outros), onde o IDP é apenas isso. A asserção de identidade (diretamente através de credenciais, ou indiretamente através de acesso implícito) é tudo o que faz. Esquemas como este vivem ou morrem pela sua capacidade de atrair uma massa crítica de partes confiantes (RP). Se não conseguirem atrair o suficiente, ou não conseguirem atrair RP que são indispensáveis para a vida online do usuário final, os esquemas de auto-confirmação terão dificuldade em acrescentar valor, e serão mais suscetíveis a atrofiar por falta de uso. Como um comentário adicional: até os sistemas do governo que são de uso praticamente obrigatória (como o sistema de autenticação do Reino Unido para declarações de impostos de renda online) pode sofrer com este problema; um ID que apenas poderá utilizar num lugar uma vez por ano, que acrescenta pouco valor, e é difícil de lembrar é fácil de ignorar.

A partir dessa perspetiva, a grande vantagem dos "IDP sociais" é que estes possuem o que é, na realidade, massa crítica automática, tanto em frequência de interação como no número de inscritos. É bem possível que interaja com o seu IDP social mais frequentemente do que com qualquer outro serviço online - até mesmo com o seu e-mail de trabalho. E um serviço como o Facebook, que se estima ter cerca de 750 milhões de usuários ativos por dia[3], oferece às RP a perspectiva de acesso a (e por) um enorme grupo de usuários com autenticação de um só clique.

Num certo sentido, é este o "chave de ouro" dos IDP. O usuário não vai lá para se autenticar, vai para fazer alguma coisa, e a autenticação é um efeito colateral conveniente. Se visitar o seu IDP significa que também pode fazer coisas em outros lugares sem ter de se voltar a autenticar, a conveniência aumenta.

Então, qual é a desvantagem? Numa palavra: panopticidade. A capacidade do seu IDP em acompanhar todos os lugares onde se autentica.

Poderá dizer que isto não é um problema novo: a panopticidade foi uma crítica feita na primeira onda madura de IDP federados [4], mas há uma pequena diferença. Nessa onda de implantações, o IDP era parte de um "círculo de confiança", com relações contratuais pré-estabelecidas entre IDP e RP, e os termos de serviço correspondente com os usuários. A razão de existir do IDP era a relação de confiança entre este e o usuário. Se confiava no seu IDP para verificar a sua identidade, provavelmente confiaria nele para não abusar dos seus dados.

Mas no modelo de "IDP social", como já estabelecido, a autenticação é essencialmente um efeito secundário. O seu modelo de negócio principal é a monetização de dados pessoais (através da agregação e revenda a anunciantes). É do interesse dos IDP sociais recolher o máximo de dados possível sobre suas atividades online, e rentabilizar esses dados. É também do interesse dos IDP sociais construir uma imagem tão abrangente

[3] http://expandedramblings.com/index.php/by-the-numbers-17-amazing-facebookstats/
[4] Os exemplos mais proeminentes são federações baseadas em SAML concebidas para especificações Liberty Alliance / OASIS

quanto possível do seu gráfico social. Isso inclui subconjuntos dos seus conhecidos que você poderia querer separados (por exemplo, contatos de trabalho e família/amigos).

Considere o seguinte: se tiver uma Google+ ID que utiliza apenas para atividade pessoal online, então, por predefinição, o Google apenas "verá" o seu gráfico social pessoal. Contudo, se o seu empregador decidir começar a utilizar a função de calendário do Google Calendar, e você tiver que se autenticar utilizando a sua Google+ ID pessoal, de repente, o Google poderá estabelecer a ligação entre os seus gráficos pessoal e profissional. O resultado, para o Google, é uma visão mais rica, mais abrangente e mais monetizável do seu gráfico social. Para você, o resultado é a erosão de uma fronteira contextual entre os seus dados pessoais e profissionais online, e isso é mau para a privacidade pessoal e autodeterminação online.

Lembre-se de que a erosão contextual não é algo com o qual concordou explicitamente, é um efeito colateral resultante da opção por usar um dos "IDP sociais". Na verdade, este gráfico social e o contexto da erosão é um fator tão importante que prefiro referir-me a ele como "gráfico dos IDP sociais». Isto também reflete o fato de um gráfico social ser extremamente difícil de forjar. É uma das formas mais estáveis de identificador comportamental (o que nos traz de volta para a nossa primeira observação contextual - que a identidade digital inclui agora identidades comportamentais, assim como identidades do tipo mais tradicional).

Conclusões

Primeiramente, as credenciais impostas por terceiros não irão desaparecer. Os governos continuarão com a necessidade de emitir credenciais sob o seu próprio controle e para os seus próprios fins (controles alfandegários, licenciamento de veículos e assim por diante). Algumas destas credenciais podem ser emitidas sob a forma de formulários, que podem ser apresentados em contextos de autenticação do setor comercial, mas o apetite para tal via parece ainda limitado, mesmo já passado um par de décadas da viabilidade técnica.

Em segundo lugar, os usuários continuarão a enfrentar uma dilema: se devem aceitar a conveniência dos "gráficos dos IDP sociais", mesmo que estes se tornem mais conscientes das desvantagens em termos de panopticidade, privacidade e auto-determinação. Lembre-se: é do interesse dos IDP de gráficos sociais que vejamos apenas a conveniência, e não os pontos negativos em termos de privacidade. Desta forma, estes poderão obter mais dados para monetizar.

Em terceiro lugar, no ecossistema de autenticação dos IDP, RP e usuários, existe um nicho para identificadores auto-confirmados e persistentes que permitam a um indivíduo (i) manter o controle sobre a identidade ou pessoa que estes escolhem para validar e (ii) criar um registo de comportamento de confiança associado a eles, e não a outra pessoa. Mas este nicho é novo e frágil: depende dos RP perceberem o valor dessas confirmações e de se congregarem em torno dos IDP em questão.

Este terceiro modelo também oferece potencial para um serviço de IDP que não seja um subproduto da monetização de dados pessoais - mas se esse não for o modelo comercial que a sustenta, qual será?