Juin 2014

Avez-vous choisi un fournisseur d'identité récemment ?

Robin Wilton
Directeur, Sensibilisation Technique Identité et Vie Privée

Internet Society

Résumé

Ce livre blanc examine le monde en mutation de la fourniture d'identité. L'identité numérique est en train d'évoluer pour passer d'un modèle « rétrospectif » à un modèle de plus en plus prédictif, basé sur des données comportementales comme l'identité traditionnel. On constate aussi un passage des informations d'identification cloisonnés vers plus assertions transférables d'identité et d'attributs.

Ces changements offrent potentiellement plus de choix et de pouvoir à l'individu, mais ce n'est qu'une potentialité. Les modèles d'identité émergents masquent aussi certains pièges, dont les utilisateurs doivent en être conscients s'ils veulent influencer le marché par des choix efficaces.

Contexte

Le monde de l'identité numérique continue d'évoluer à un certain rythme. Le concept d'identité numérique proprement dit englobe maintenant plusieurs formes différentes, principalement les trois suivantes :

- les identités « rétrospectives » traditionnelles, où vous passez par un processus d'inscription fiable pour recevoir d'un tiers un justificatif d'identité que vous pourrez présenter plus tard pour vous authentifier ;
- les identités « auto-certifiées » peu fiables, où le tiers fait un peu plus que vous fournir un identifiant correct du point de vue syntaxique et qu'il confirmera quand on le lui demandera ;
- les identités « comportementales », où les fournisseurs de services recueillent suffisamment de données sur une personne pour révéler que cette même personne visite un site donné à maintes reprises.

Signalons que le troisième type d'identification (comportementale) n'exige pas forcément d'action explicite de la part de l'utilisateur. Si un site Web place un témoin de navigateur, ou récupère votre adresse Internet (IP), cela suffit pour constituer la base d'une identité comportementale – bien qu'il existe aussi d'autres moyens plus sophistiqués d'y parvenir.

Les fournisseurs d'identité (IdPs) ont évolué eux aussi et continuent de le faire. Le premier IdP que rencontrent la plupart des utilisateurs fait probablement partie de l'un des trois types suivants :

- le gouvernement (en particulier dans le cas des justificatifs d'identité non numériques tels que les passeports, permis de conduire, etc.) ;
- un établissement scolaire (qui délivre une carte d'étudiant pour l'accès en ligne aux ressources destinées aux étudiants, aux bibliothèques, aux réseaux, etc.) ;

> un employeur (qui délivre des identifiants pour accéder aux comptes de messagerie, aux applications d'entreprise, etc.).

Pour généraliser/simplifier légèrement le concept, disons que tous ces IdP délivrent des justificatifs d'identité cloisonnés. Vous ne pourrez probablement pas utiliser un justificatif d'identité délivré par le gouvernement pour vous connecter aux systèmes de votre employeur (sauf si, bien sûr, ils constituent un seul et même système ; mais il s'agit là d'un cas particulier). La carte d'étudiant que vous avez utilisée pendant vos études universitaires ne fonctionnera probablement pas non plus sur les systèmes de votre employeur. Comme je le disais, il s'agit là d'une simplification. Les systèmes d'identité fédérés relient les systèmes cloisonnés. Il est toutefois plus fréquent que les fédérations limitent leur champ d'application au contexte de l'enseignement supérieur, au contexte du gouvernement ou à une identification unique dans toutes les organisations commerciales[1].

Choix

Ces trois exemples partagent une autre caractéristique marquante : En tant qu'utilisateur, vous n'avez pas ou peu de choix en la matière. Si vous vous inscrivez dans une université ou décrochez un emploi, vous n'aurez probablement pas d'autre option que d'adhérer au service d'identification qui vous est offert ou d'imaginer travailler sans avoir accès aux ressources en ligne (ce qui, de nos jours, est souvent impossible).

Pour avoir le choix, vous avez deux solutions. Premièrement, avec l'apparition des systèmes tels qu'OpenID et OAuth, les utilisateurs peuvent désormais certifier eux-mêmes qu'ils sont propriétaires d'une ressource (p. ex. une adresse électronique ou un compte en ligne). Ainsi, ils affirment implicitement leur identité.

Deuxièmement, des systèmes tels que « Web of Trust » de Thawte (aujourd'hui malheureusement abandonné) ou le nouveau UnitedID[2] cherchent à offrir aux utilisateurs un justificatif d'identité permanent associé à un identifiant auto-certifié (comme une adresse électronique ou un jeton d'authentification). UnitedID est particulièrement intéressant, dans la mesure où il vise à fournir une identité en ligne fiable au consommateur du marché de masse, sans avoir recours au modèle commercial commun et financé par la publicité de fourniture de services en ligne.

Il est possible que ce justificatif d'identité ne soit pas intrinsèquement fiable. À la base, cela dépendra de la fiabilité du processus d'inscription. S'il m'est trop facile d'obtenir un

[1] Il existe des exceptions notables, comme le système scandinave BankID, qui comble le fossé entre le secteur commercial et public et les fédérations de l'industrie aérospatiale et de la défense, où les interactions entre les organismes gouvernementaux et leurs sous-traitants sont nombreuses.

[2] Page d'accueil de UnitedID : http://unitedid.org/about/

justificatif d'identité valable du point de vue syntaxique disant que je suis Grace Kelly, l'utilité du système sera restreinte. Toutefois, si le justificatif d'identité est suffisamment constant, il importe peu qu'il me fasse passer pour Grace Kelly : au fil du temps, un identifiant permanent peut « accumuler » de la fiabilité de la même manière qu'un être humain qui adopte une conduite digne de confiance en tout temps et accumule ainsi de bons comportements.

Mais attention : N'y a-t-il pas une autre catégorie d'IdP qui donne le choix aux utilisateurs et leur permet de s'authentifier auprès de nombreux fournisseurs de services différents ? Dans un sens, oui. Si vous avez déjà accepté de vous connecter au service X en utilisant votre identifiant Google, Facebook ou Twitter (pour ne citer que quelques-unes des options habituelles), alors vous avez « acquis » un IdP par défaut, sans l'avoir jamais choisi délibérément. Du moins dans un sens. Il serait peut-être plus exact de dire que vous avez choisi d'utiliser un IdP qu'on a présélectionné pour vous. Pour l'instant, je les appellerai « IdP sociaux ». Ils ont des répercussions sur la protection de votre vie privée que vous devriez soigneusement examiner…

Répercussions

J'ai évoqué plus haut l'option d'auto-certification (OpenID, OAuth, UnitedID et autres), qui renvoie à l'IdP en tant que tel. La certification d'identité (directement via des justificatifs d'identité, ou indirectement via un accès implicite) se limite à cela. La survie ou la disparition de systèmes comme celui-ci dépend de leur capacité à attirer une masse critique de parties utilisatrices (RP). S'ils ne peuvent pas en attirer assez, ou ne parviennent pas à attirer les RP indispensables à la vie en ligne de l'utilisateur final, les systèmes d'auto-certification auront du mal à offrir une valeur ajoutée et pourraient s'atrophier, par manque d'utilisation. Soit dit en passant : même les systèmes gouvernementaux qu'il est pratiquement obligatoire d'utiliser (comme le système d'authentification du Royaume-Uni pour les déclarations de revenus en ligne) peuvent souffrir de ce problème ; un identifiant que vous ne pouvez utiliser qu'à un seul endroit, une fois par an, n'apporte que peu de valeur ajoutée. Il est difficile de s'en souvenir, mais facile de l'ignorer.

De ce point de vue, le grand avantage des « IdP sociaux » est qu'ils disposent effectivement d'une masse critique automatique, à la fois dans la fréquence des interactions et dans le nombre de personnes inscrites. Il est tout à fait possible que vous interagissiez avec votre IdP social plus souvent qu'avec tout autre service en ligne, même votre messagerie professionnelle. Un service comme Facebook, qui compterait environ 750 millions d'utilisateurs actifs quotidiens[3], offre aux RP la perspective d'accéder à un énorme groupe d'utilisateurs, qui y accède en retour, et ce, en un seul clic.
Dans un sens, c'est le Graal des IdP. Vous n'y allez pas pour vous authentifier : vous y allez pour autre chose ; l'authentification est un effet secondaire bien pratique. Si, en

[3] http://expandedramblings.com/index.php/by-the-numbers-17-amazing-facebookstats/

consultant votre IdP, vous pouvez aussi mener d'autres actions ailleurs, sans avoir à vous ré-authentifier, vous gagnez encore en simplicité.

Alors, quel est l'inconvénient ? En un mot : Panoptique. C'est-à-dire la capacité de votre IdP à surveiller tous les endroits où vous vous authentifiez.

Vous me répondrez peut-être que le problème n'est pas nouveau : La « Panoptique » était une critique adressée à la première vague mature d'âge d'IdP fédérés à ce sujet[4]. Mais il y a une légère différence. Dans cette vague de déploiements, l'IdP faisait partie d'un « cercle de confiance », avec les relations contractuelles préétablies entre les IdP et les RP et les conditions d'utilisation correspondantes avec les utilisateurs. La raison d'**ê**tre de l'IdP était la relation de confiance qu'il avait nouée avec l'utilisateur. Si vous avez fait confiance à votre IdP pour qu'il vérifie votre identité, vous serez probablement sûr qu'il n'abusera pas de vos données.

Mais dans le modèle de l'« IdP social » susmentionné, l'authentification est avant tout un effet secondaire. Son modèle économique principal est la monétisation des données personnelles (par le biais de l'agrégation et de la revente aux publicitaires). C'est dans l'intérêt de l'IdP social de recueillir autant de données que possible sur vos activités en ligne, avant de les monétiser. L'IdP social a également intérêt à construire une image aussi complète que possible de votre graphe social, notamment des sous-ensembles de vos connaissances que vous souhaiteriez peut-être autrement séparer (p. ex. les contacts de travail d'un côté et la famille/les amis de l'autre).

Considérez ceci: Si vous avez un identifiant Google+ que vous utilisez uniquement pour vos activités personnelles en ligne, alors, par défaut, Google « verra » seulement votre graphe social personnel. Toutefois, si votre employeur décide un jour d'externaliser la gestion d'agenda sur Google Agenda, et que vous devez vous authentifier en utilisant votre identifiant personnel Google+, alors Google pourra subitement faire le lien entre vos graphes personnel et professionnel. Résultat ? Google profitera d'une vision plus riche, plus complète et plus « monétisable » ou commercialisable de votre graphe social.
Quelle conséquence pour vous ?
La limite contextuelle entre vos données en ligne personnelles et professionnelles s'érode, ce qui nuit au respect de votre vie privée et à votre capacité d'autodétermination en ligne.

Rappelez-vous que vous n'avez pas explicitement accepté cette érosion contextuelle. Il s'agit d'un effet secondaire lorsque vous optez pour l'un des « IdP sociaux ». En fait, ce graphe social et cette érosion contextuelle sont tellement déterminants que je préfère parler d'« IdP du graphe social ». L'expression traduit aussi l'immense difficulté à falsifier un graphe social. Il s'agit de l'une des formes les plus stables de l'identifiant

[4] Les exemples les plus importants étant les fédérations basées sur SAML, conçues pour les spécifications Liberty Alliance/OASIS

comportemental (ce qui nous ramène à notre observation contextuelle du début : l'identité numérique inclut désormais les identités comportementales et les identités plus traditionnelles).

Conclusions

Premièrement, les justificatifs d'identité imposés par des tiers ne vont pas disparaître. Les gouvernements auront encore besoin d'émettre des justificatifs d'identité sous leur propre contrôle et à leurs propres fins (contrôles aux frontières, immatriculation des véhicules, etc.). Il est possible que certains de ces justificatifs d'identité soient présents sous des formes utilisables à une échelle commerciale, mais manifestement, l'intérêt qu'ils soulèvent est encore limité, même après plusieurs décennies de viabilité technique.

Deuxièmement, les utilisateurs devront encore accepter ou refuser de passer par les « IDP du graphe social » si pratiques, même s'ils ont davantage conscience des inconvénients, en termes de panoptique, de respect de la vie privée et d'autodétermination. N'oubliez pas : Dans l'intérêt des IDP de graphe social, vous ne devez percevoir que le côté pratique, et pas le problème lié à la confidentialité. De cette façon, ils obtiennent plus de données personnelles à monétiser.

Troisièmement, dans l'écosystème d'authentification rassemblant les IDP, les RP et les utilisateurs, il existe un créneau pour les identifiants auto-déclarés et permanents. Ces derniers permettent à une personne (i) de garder le contrôle sur l'identité ou l'image qu'elle choisit de revendiquer, et (ii) d'adopter une conduite fiable en permanence, qu'on lui attribue en toute confiance, plutôt qu'à quelqu'un d'autre. Mais ce créneau est nouveau et fragile : il dépend de la perception de la valeur de ces affirmations par les RP et de leur regroupement autour des IDP en question.

Ce troisième modèle offre également la possibilité d'un service IDP qui ne soit pas un produit dérivé de la monétisation des données personnelles. Mais si ce n'est pas le modèle commercial qui le soutient, qui le fera ?