Qu'est-ce qu'un service d'identité

Stéphane Bortzmeyer
AFNIC
bortzmeyer@nic.fr

13 janvier 2009

L'identité fait du bruit

1. Comment je fais pour me souvenir de tous mes mots de passe ?
2. Amazon.com peut-il corréler mes achats de DVD en ligne avec mes déplacements en métro faits avec une carte Navigo ?
3. Quels sont les avantages et les inconvénients de commenter sur un blog avec un pseudonyme et pas avec mon nom de l'état civil ?
4. ...

Dans les bibliothèques

1. Contrôle d'accès physique,
2. Contrôle d'accès à des applications Web (documents en diffusion restreinte, par exemple),
3. Accès à des applications distantes,
4. Et aussi l'identité des objets, de leur ISBN à la puce RFID.

Service d'identité et identité

L'**identité** est une notion trop philosophique pour cet exposé :-)

Un **service d'identité** est une notion pratique et donc plus apte à être étudiée.

Conséquence : on ne cherche pas à définir la **vraie** identité ou bien l'identité officielle. L'identité devient plurielle.

Proposition de définition

Un service d'identité, c'est :

1. Attribuer un identificateur (ce qui implique en général un registre, pour que l'identificateur soit unique),
2. Authentifier l'utilisateur ou la ressource qui prétend être désigné par cet identificateur,
3. Servir des données sur cet utilisateur ou cette ressource (son nom, son âge, son pays, sa langue),
4. Servir des données externes, à partir d'autres sources,
5. Servir des autorisations sur ce que l'utilisateur a le droit de faire ou pas.

1) Identificateurs, exemples

- 160109940400823,
- Jeanne Durand, née à Chapelle-des-Bois le 1er février 1953,
- `http://www.bortzmeyer.org/` (avec OpenID, c'est un identificateur d'une personne),
- `bortzmeyer@gmail.com` (avec Jabber/XMPP, c'est un identificateur)
- `http://fr.wikipedia.org/Wiki/Simone_de_Beauvoir` (identificateur d'une ressource, ici un article biographique)
- `978-0-19-507993-7`

Qui attribue les identificateurs ?

Un ou plusieurs registres, aux pratiques parfois contestables (DOI. . .).

Qui dit identité dit souvent **fournisseur d'identité** (l'État, Google, Microsoft, Verisign ou les autres Autorités de Certification X.509, . . .).

Confiance dans les fournisseurs ?

Avez-vous déjà vérifié la liste des Autorités de Certification que Microsoft ou Mozilla ont installé d'autorité dans votre navigateur ?

Vous faites confiance à l'Association des Notaires Argentins ?

Ou bien au gouvernement de Taïwan ?

Ou bien à RapidSSL qui, en décembre 2008, utilisait encore MD5, technique cassée depuis des années ?

Qu'est-ce que fait un fournisseur d'identité ?

Prenons l'exemple de la vie quotidienne d'une Autorité de Certification (CA) X.509.

1. Stocker ses clés en un endroit très sûr,
2. Avoir des procédures pour changer les clés de temps en temps (et pour les grosses tuiles),
3. Vérifier les identités, selon des critères qui dépendent de la CA,
4. Signer les demandes de certificat.

2) Authentifier

« Sur Internet, on ne voit pas du premier coup d'œil que vous êtes un chien. »

- Document d'identité officiel, comme la Carte Nationale d'Identité. Pas pratique sur l'Internet.
- Avec OpenID, l'authentification est sous-traitée à un système tiers, nommé l'OP (OpenID Provider).
- Signatures cryptographiques comme PGP ou X.509.

Attention, authentification n'est pas autorisation.

3) Servir des données

Un service d'identité permet souvent d'accéder à des données sur l'utilisateur, et parfois des données sensibles.

Exemple : si vous avez un nom de domaine comme `bortzmeyer.org`, le service **whois** du registre (l'organisme qui gère la base) donne parfois des informations bien indiscrètes au public.

Certains registres permettent de restreindre la diffusion des données (mais lisez bien les petites lettres du contrat). C'est le cas avec `bortzmeyer.fr`.

4) Accéder à des données externes

Avec un identificateur bien choisi, on peut facilement faire des **jointures** entre services d'identité différents et croiser des fichiers.

Sans un bon identificateur, cela reste possible, avec diverses heuristiques. Par exemple, il est souvent possible de mettre un nom sur les entrées d'un fichier pseudonymisé.
`http://www.wired.com/politics/security/commentary/securitymatters/2007/12/securitymatters_1213`

5) Servir des autorisations

Les autorisations sont une forme particulière de données.

Exemple de différence entre authentification et autorisation : la lutte contre le spam. Si mon adresse `stephane@bortzmeyer.fr` est authentifiée, suis-je pour autant autorisé à transmettre du courrier proposant du Viagra ?

Les délinquants, eux aussi, ont des papiers d'identité. Authentifier n'est pas suffisant. Il faut aussi des systèmes d'**accréditation** ou de **réputation**.

Un peu de technique

- Cryptographie : par des opérations mathématiques, on peut prouver que tel message a été signé par le possesseur d'une **clé** numérique. À la base de techniques comme TLS, X.509, PGP, ...
- X.509 : norme de certificats cryptographiques. C'est ce qu'utilise votre navigateur Web pour afficher le petit cadenas.
- TLS (ex-SSL) : le protocole d'échange de données chiffrées entre votre navigateur et le site Web.
- OpenID : une des propositions pour un identificateur multi-sites sur le Web. La vérification est sous-traitée à un fournisseur d'identité (OP pour *OpenID provider*).
- Carte d'Identité Électronique : carte munie d'un processeur stockant la clé privée et permettant la signature et donc l'authentification.
- Shibboleth : mécanisme d'identité utilisé notamment par la Fédération d'identité gérée par le Comite Réseau des Universités. Cela permet à un employé d'une université d'accéder aux ressources privées d'une autre, sans avoir de

La sécurité est un processus, pas un produit

Les problèmes de sécurité ne sont pas prioritairement techniques

Dans tous les cas, la technique ne résout pas tout : il existe toujours des failles (« ce système est parfaitement sûr ») et la technique peut être tellement complexe qu'elle est sous-utilisée (cas de la cryptographie).

Questions philosophiques

Ai-je une identité ou plusieurs ?

Je considère que l'identité n'est pas intrinsèque à une entité. Une personne physique, par exemple, a d'autres identités que celle que l'État lui attribue.

Il est important que l'identité soit maîtrisée par l'utilisateur, pas par un tiers, même lorsque ce dernier affirme que « toutes les précautions ont été prises.

Anonymat et pseudonymat

« Anonyme » devrait n'être utilisé que lorsqu'il n'y a pas d'identificateur du tout. C'est rare sur Internet ! (*Cookies*, adresses IP, . . .).

« Pseudonyme » laisse entendre qu'il existe des identificateurs moins bons que d'autres.

Il vaut mieux se méfier de ces termes et parler d'identités multiples.

Questions politiques et juridiques

Des lois comme la loi Informatique & Libertés posent des principes politiques comme le fait que certains droits liés à l'identité sont inaliénables.

Et le droit à l'« anonymat » ?

Et à la multiplicité des identités ?

Ne devraient-ils pas faire partie des droits de base de l'utilisateur des NTIC ?