Génération hors ligne d'attributs certifiés et de pseudonymes certifiés à chaînabilité contrôlée

Yves Deswarte[1,2]

[1] CNRS, LAAS, 7 avenue du Colonel Roche, F-31400 Toulouse, France
[2] Université de Toulouse, LAAS, F-31400 Toulouse, France
yves.deswarte@laas.fr

Introduction

Le cyber-espace prend une place de plus en plus importante dans notre vie de tous les jours, en particulier avec le commerce en ligne, les réseaux sociaux, la diffusion de contenus gratuits ou payants, etc. Tous ces usages reposent sur une confiance, le plus souvent implicite, entre des partenaires qui ne se connaissent pas et qui ne se rencontreront probablement jamais dans le monde réel. Cette confiance est trop souvent bafouée ou abusée par des délinquants ou des criminels. Comment être sûr que la personne qui *tchatte* avec votre enfant est bien une jeune fille de 13 ans habitant dans le voisinage, et non pas un vieux pervers barbu ? Comment être sûr que le contenu auquel vous accédez est bien authentique et que sa distribution est légale ? Les informations publiées sur Twitter sont-elles vraiment crédibles ? L'identité de votre correspondant a-t-elle été usurpée ? Les membres d'une communauté virtuelle sont-ils dignes de confiance ?

Pour améliorer ou justifier cette confiance nécessaire, on veut nous imposer des mécanismes de sécurité, comme l'authentification forte et la traçabilité des communications et des contenus, qui sont autant d'atteintes à la vie privée : elles facilitent la collecte et le croisement d'informations personnelles, dont la validité est garantie par ces moyens de sécurité. Il convient donc de développer d'autres techniques, préservant la vie privée tout en permettant d'avoir une confiance justifiée dans certaines informations critiques. Comme les autres technologies de protection de la vie privée (*Privacy-Enhancing Technologies*, ou *PETs*), ces techniques doivent être basées sur deux principes fondamentaux : la minimisation des données personnelles (ne diffuser que les données indispensables), et la souveraineté sur ces données (chacun garde le contrôle sur l'usage qui peut être fait de ses données personnelles).

Dans cet article, nous proposons deux moyens pour améliorer cette confiance : les attributs certifiés et les pseudonymes certifiés. "*Certifiés*" veut dire garantis par une autorité digne de confiance, sans pour autant dévoiler l'identité des personnes auxquelles ils correspondent. Pour garantir la souveraineté, il faut que ces attributs ou pseudonymes certifiés soient générés "hors ligne", c'est-à-dire sans connexion avec l'autorité certifiante, sinon la simple observation de la connexion dévoilerait des informations sensibles (la création d'un attribut ou d'un pseudonyme). Il faut en plus que l'utilisateur puisse en contrôler la *chaînabilité*, c'est-à-dire pouvoir décider d'utiliser des attributs et des pseudonymes différents quand il le souhaite, et que personne (sauf l'autorité certifiante) ne puisse identifier la personne à laquelle ils correspondent, ni même distinguer s'ils correspondent ou non à la même personne. Enfin, pour garantir l'authenticité de ces attributs ou pseudonymes, ils ne doivent pas être falsifiables ou transférables (volontairement ou non) à quelqu'un d'autre qui les utiliserait à son compte (usurpation). Ils doivent aussi permettre d'en contrôler la "*fraîcheur*", c'est-à-dire d'en empêcher le rejeu.

Un attribut certifié permet, par exemple, de prouver qu'on a plus (ou moins) de 18 ans, qu'on est domicilié dans une région, une commune, ou un quartier donnés, qu'on est membre d'une certaine

association, voire qu'on possède un permis de conduire en cours de validité, *etc*., sans pour autant dévoiler d'autre information sur son identité. Un pseudonyme certifié permet de se faire connaître comme étant la même personne dans différents échanges, sans pour autant dévoiler aucune information sur son identité. Pour punir les abus ou les fraudes commis à l'aide de ces attributs ou pseudonymes certifiés, ceux-ci contiennent une information qui permet à l'autorité certifiante d'identifier avec certitude la personne qui y correspond. Il suffit alors à la victime de la fraude ou de l'abus de présenter la preuve de la fraude ou de l'abus, accompagnée de l'attribut ou du pseudonyme certifié, à l'autorité certifiante pour que celle-ci lève l'anonymat du malfaiteur. Ceci doit être suffisamment dissuasif pour rendre impraticables ces fraudes ou abus, et donc améliorer la sécurité et donc la confiance. Il est à noter que dans ce schéma, contrairement aux techniques de sécurité habituellement proposées ou même rendues obligatoires par certaines législations liberticides, il est inutile d'identifier et de tracer les innocents, seuls les coupables sont surveillés.

Exemples d'utilisation

- L'âge peut être un attribut certifié (avec différentes granularités possibles : mineur/majeur, moins de 12 ans, plus de 60 ans, *etc*.). Ainsi, il serait facile d'implémenter un *contrôle parental* efficace au niveau des serveurs, plutôt que comme aujourd'hui sur la machine *cliente*, trop facile à contourner. Cela permettrait aussi de justifier des droits à réduction (pour les enfants, ou pour les personnes âgées), de garantir son âge dans des réseaux sociaux, des *chats*, ou autres, sans dévoiler son identité.
- La nationalité peut aussi être un attribut certifié, qui devrait suffire au passage de frontière, mais aussi pour implémenter des privilèges ou des interdictions liées à la nationalité. On se souvient par exemple de la vente d'objets nazis sur eBay.
- Le domicile peut aussi être un attribut certifié, avec différents niveaux de granularité : bâtiment, quartier, commune, département, région, pour obtenir des privilèges ou des réductions liées au domicile : par exemple, l'accès à une bibliothèque municipale en ligne, la consultation d'informations administratives, la participation à une consultation des habitants d'un quartier, des réservations à tarif réduit pour un spectacle, des abonnements d'accès à des équipements sportifs municipaux, *etc*.
- La détention d'un permis de conduire, l'inscription comme employeur à l'URSSAF, ou autres caractéristiques administratives, peuvent être des attributs certifiés suffisants pour prouver des droits sans pour autant devoir décliner son identité.
- L'adhésion à une association, l'abonnement à des services en ligne (par exemple, pour la consultation de journaux), peuvent être des attributs certifiés permettant l'accès à des services en ligne réservés aux membres ou aux abonnés.
- L'utilisation de pseudonymes certifiés permettrait à chacun d'appartenir à différents réseaux sociaux ou communautés virtuelles sans déclarer son identité, et sans que ces différentes appartenances ne puissent être reliées à une même personne. Associé à des moyens de paiements anonymes (probablement à anonymat révocable), et des moyens de livraison adaptés (points relais), il serait possible de participer anonymement au commerce électronique.
- L'utilisation de pseudonymes certifiés permettrait aussi d'identifier des fournisseurs de contenus illégaux ou autres cyber-malfaiteurs, sans devoir ficher et tracer les connexions des gens honnêtes, comme c'est aujourd'hui rendu obligatoire par une législation excessive et mal adaptée.

Implémentations possibles

Pour pouvoir générer des attributs ou pseudonymes certifiés hors ligne qui soient infalsifiables et intransférables, il faut disposer d'un objet personnel, comme une carte d'identité électronique, contenant les informations nécessaires (attributs, informations de certification fournies par l'autorité) et les moyens cryptographiques permettant de générer les attributs et pseudonymes certifiés. Cet objet personnel (typiquement une carte à puce) doit être activée par la reconnaissance biométrique de son détenteur, cette reconnaissance étant réalisée par la carte elle-même (*Match-On-Card*), plutôt que par le terminal dans lequel on insère la carte, de façon à éviter que les caractéristiques biométriques ne soient transmises au terminal. Les attributs et pseudonymes certifiés doivent être signés par des moyens cryptographiques, de façon à permettre d'identifier l'autorité qui a produit la carte, sans pour autant fournir des informations traçables et identifiables liées à la carte (une clé de signature permanente, par exemple). Ils doivent aussi contenir des informations prouvant la fraîcheur de la génération des attributs et pseudonymes (par horodatage certifié, ou par protocole cryptographique avec défi).

Cette fonction de génération d'attributs et de pseudonymes certifiés devrait pouvoir assez facilement être introduite dans la *carte nationale d'identité préservant la vie privée* (CNIPVP) que nous avons proposée [1,2,3,4], puisqu'elle possède déjà certaines briques cryptographiques de ce genre. Dans notre vision, la CNIPVP est produite par une autorité régalienne dépendant de l'État, comme les cartes d'identité traditionnelles.

Ceci ne serait pas satisfaisant pour certaines utilisations, par exemple l'adhésion à une association ou l'abonnement à un service. Dans ce cas, la carte à puce pourrait être fournie et mise à jour par un tiers de confiance faisant office d'autorité certifiante multi-services, ce qui pourrait développer un nouveau marché lié à la gestion d'identité préservant la vie privée. On pourrait même imaginer fusionner ce service avec des services de paiement en ligne comme PayPal.

Conclusion

Les attributs certifiés et les pseudonymes certifiés pourraient devenir des moyens essentiels pour protéger la vie privée et améliorer la sécurité du cyber-espace. Ils pourraient aussi rendre inutiles et obsolètes les moyens de surveillance des gens honnêtes, sans pour autant fournir d'impunité aux délinquants ou criminels.

Remerciements

L'auteur remercie par avance Sébastien Gambs et Carlos Aguilar pour l'aide qu'ils lui apporteront à la réalisation d'un prototype mettant en œuvre ce schéma dans une CNIPVP, grâce en particulier à leurs grandes compétences en cryptographie.

Références

[1] Yves DESWARTE, Sébastien GAMBS, « Une carte nationale d'identité préservant la vie privée (CNIPVP) », Atelier sur *la protection de la vie privée*, INRIA-CNRS, Annecy, 25-27 mai 2010. http://licit.inrialpes.fr/apvp2010/

[2] Yves DESWARTE, Sébastien GAMBS, « A Proposal for a Privacy-preserving National Identity Card », *Transactions on Data Privacy*, ISSN: 1888-5063, vol.3(3), décembre 2010, pp.253-276. http://www.tdp.cat/issues/abs.a060a10.php

[3] Yves DESWARTE, Sébastien GAMBS, Moussa TRAORÉ, « Démonstration d'une carte nationale d'identité préservant la vie privée », Atelier sur *la protection de la vie privée*, Sorèze, 20-22 juin 2011. http://homepages.laas.fr/mkilliji/APVP2011/Site/Programme_files/Article_10.pdf

[4] Yves DESWARTE, Sébastien GAMBS « The Challenges Raised by the Privacy-Preserving Identity Card », in *Cryptography and Security*: *From Theory to Applications — Festschrift Jean-Jacques Quisquater* (D. Naccache, Ed.), Springer, mars 2012, LNCS 6805, ISBN 978-3-642-28367-3, pp.383-404. http://www.springer.com/computer/security+and+cryptology/book/978-3-642-28367-3