Principes et technologies de protection de la vie privée sur l'Internet

Yves Deswarte
deswarte@laas.fr

LAAS-CNRS, Toulouse

Sommaire

- Définitions
- Principes de base
- PETs : Privacy Enhancing Technologies
  - Communications et accès anonymes
  - Gestion d'identités multiples
  - Autorisation respectant la vie privée
  - Gestion des données personnelles
- Projet Prime

"Privacy" : définitions

- Intimité, respect/protection de la vie privée
- Critères Communs (ISO 15408) :
  une classe de fonctionnalité, 4 propriétés :
  - Anonymat : garantit qu'un utilisateur peut utiliser une ressource ou un service sans révéler son identité d'utilisateur
  - "Pseudonymat" : idem, sauf que l'utilisateur peut quand même avoir à répondre de cette utilisation
  - "Non-chaînabilité" : garantit qu'un utilisateur peut utiliser plusieurs fois des ressources ou des services sans que d'autres soient capables d'établir un lien entre ces utilisations
  - Non-observabilité : garantit qu'un utilisateur peut utiliser une ressource ou un service sans que d'autres, en particulier des tierces parties, soient capables d'observer que la ressource ou le service est en cours d'utilisation

Pseudonymat < anonymat < non-chaînabilité < non-observabilité

1er Principe pour protéger la vie privée :

- "Souveraineté" : garder le contrôle sur ses [méta-]données personnelles

-> stockage sur un dispositif personnel (carte à puce, PDA, PC…)

-> si ces données sont divulguées à un tiers, imposer des **obligations** sur leur usage

- Date de péremption
- Notification en cas de transfert ou d'usage non prévu
- etc.

2ème Principe pour protéger la vie privée :

- Minimisation des données personnelles

ne transmettre une information qu'à ceux qui en ont besoin pour réaliser la tâche qu'on leur confie
-> "Besoin d'en connaître" ("*need-to-know*")

puis destruction/oubli

- … dans le "cyber-espace" comme dans le monde réel

- …avec des limites : certaines informations personnelles doivent pouvoir être fournies aux autorités judiciaires en cas de litige ou d'enquête (lutte contre le blanchiment d'argent sale, par exemple) : "pseudonymat" plutôt qu'anonymat total

- Liens : minimisation <--> proportionnalité et finalités légitimes

Exemple : commerce électronique (1)

- Parties impliquées :
  un client, un marchand, un service de livraison, des banques, un émetteur de carte de crédit, un fournisseur d'accès Internet, …

- Le marchand n'a pas besoin (en général) de l'identité du client, mais doit être sûr de la validité du moyen de paiement.

- La société de livraison n'a pas besoin de connaître l'identité de l'acheteur, ni ce qui a été acheté (sauf les caractéristiques physiques), mais doit connaître l'identité et l'adresse du destinataire.

Exemple : commerce électronique (2)

- La banque du client ne doit pas connaître le marchand ni ce qui est acheté, seulement la référence du compte à créditer, le montant …
- La banque du marchand ne doit pas connaître le client…
- Le f.a.i. ne doit rien connaître de la transaction, sinon les caractéristiques techniques de la connexion …

PET : Privacy-Enhancing Technology

- Communications et accès anonymes
- Gestion d'identités multiples
- Autorisation respectant la vie privée
- Gestion des données personnelles

Adresse IP= "donnée identifiante"

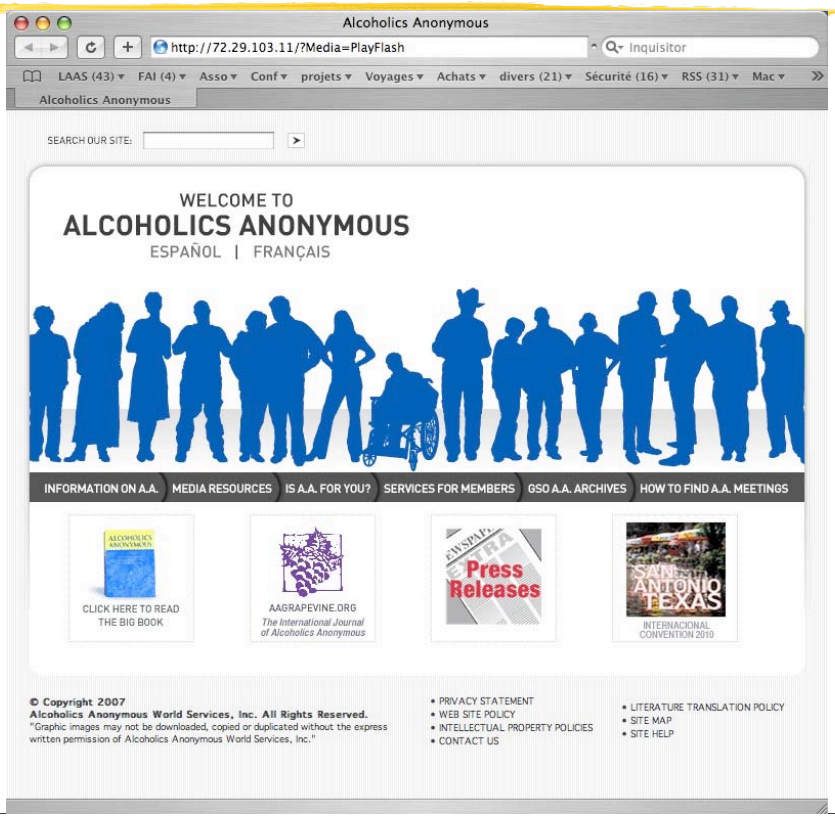
Exemple :

```
Return-Path: <Yves.Deswarte@laas.fr>
Received: from laas.laas.fr (140.93.0.15) by mail.libertysurf.net
(6.5.026)
      id 3D518DEF00116A4D for yves.deswarte@libertysurf.fr; Tue, 13 Aug
2002 13:44:40 +0200
Received: from [140.93.21.6] (tsfyd [140.93.21.6])
    by laas.laas.fr (8.12.5/8.12.5) with ESMTP id g7DBid1D001531
    for <yves.deswarte@libertysurf.fr>; Tue, 13 Aug 2002 13:44:39 +0200
(CEST)
User-Agent: Microsoft-Entourage/10.1.0.2006
Date: Tue, 13 Aug 2002 13:44:38 +0200
Subject: test
From: Yves Deswarte <Yves.Deswarte@laas.fr>
To: <yves.deswarte@libertysurf.fr>
Message-ID: <B97EBDC6.2052%Yves.Deswarte@laas.fr>
Mime-version: 1.0
Content-type: text/plain; charset="US-ASCII"
Content-transfer-encoding: 7bit
```

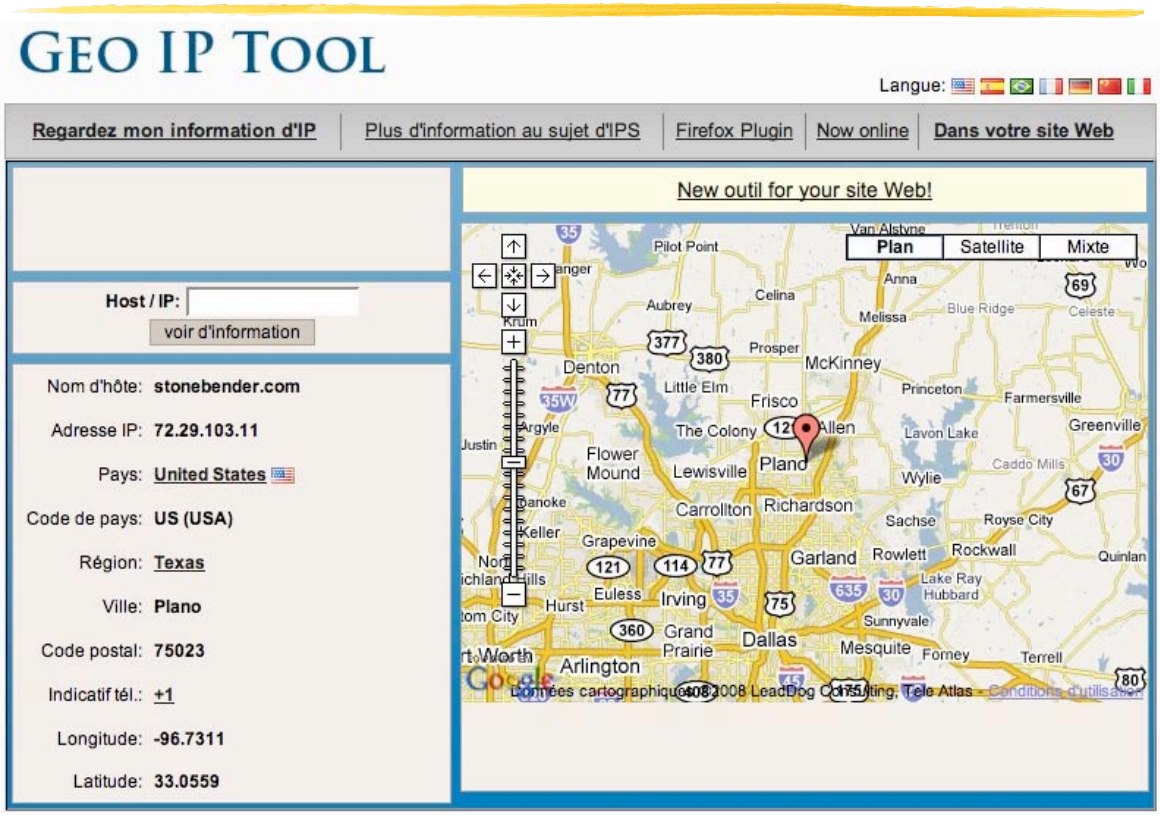
Adresse IP= "info sensible"

Exemple :

http://72.103.29.11



Adresse IP= localisation



IP V6, réseaux ad hoc, …

- Demain : IP partout (*pervasive/ubiquitous computing, intelligence ambiante, sensor networks, RFID, convergence 4G …*)
- chaque "machin" aura une adresse IP implicite *unique et permanente* (basée sur un numéro de fabrication)
- chaque personne aura plusieurs machins …
- … qui se connecteront aux machins proches (réseaux ad hoc)
- … qui s'identifieront, routeront leurs communications, fourniront des infos contextuelles, etc.

1° PET : Communications anonymes

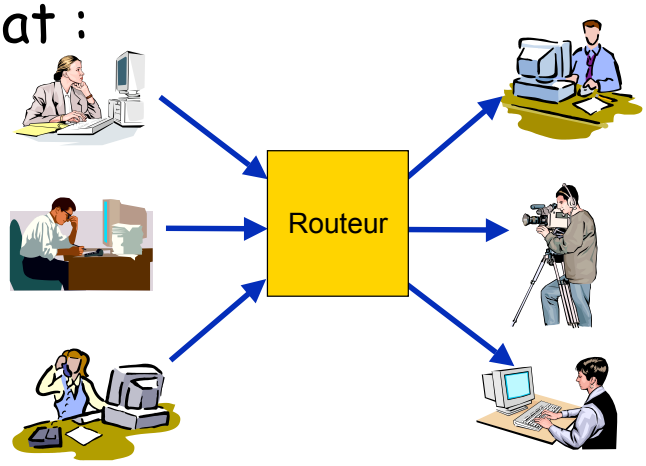
Supprimer le lien utilisateur - adresse IP :

- affectation dynamique des adresses IP (DHCP, PPP, NAT, ...)
- Routeurs d'anonymat :

  MIX

  Onion Routing (TOR)

  Crowds (P2P)



1bis PET: Accès anonyme à des services

- Relais d'anonymat (*anonymity proxy*) : unidirectionnels ou bidirectionnels
  - e-mail, news (Usenet)
    - anon.penet.fi (700 000 utilisateurs en 1996 !)
    - Cypherpunks
  - ftp
  - Web : ex: proxify.com
  - ...
- Serveur de pseudonymes :
  - e-mail
  - Identités multiples fournies par des f.a.i. (adresses mél)

2° PET : gestion d'identités multiples

- Identité = représentation d'une personne physique
- Réduire/contrôler les liens entre une personne et les données (et méta-données) la concernant (contrôler la *chaînabilité*)
  - on présuppose la non-chaînabilité des communications et des accès
- Mais : accès personnalisés / privilégiés : pseudonymes
  - Préférences (ex: météo)
  - "Rôles" différents -> pseudonymes différents
    - Ex: contribuable et électeur
  - Durée de vie liée aux besoins de chaînabilité
    -> pseudonymes "jetables"
  - Authentification adaptée au risque d'usurpation d'identité (et à la responsabilité)
- Identités virtuelles multiples vs. "single-sign-on"
  Liberty Alliance <http://www.projectliberty.org>
  vs. Microsoft Passport

3° PET: Autorisation

- Aujourd'hui sur Internet : client-serveur
  le serveur accorde ou refuse des privilèges au client en fonction de son identité déclarée (éventuellement vérifiée par des mécanismes d'authentification)
- Le serveur doit enregistrer des données personnelles : preuves en cas de litige
- Ces données peuvent être utilisées à d'autres fins (profilage des clients, marketing direct, revente de fichiers clients, chantage…)
- Action P3P (W3C) : *Platform for Privacy Preferences Project*
  vérification automatique de politiques de sécurité/privacy "déclarées"

Ce schéma est dépassé

- Les transactions sur Internet mettent en jeu généralement plus de deux parties (ex : commerce électronique)
- Ces parties ont des intérêts différents (voire opposés) : suspicion mutuelle
- Nocif pour la vie privée : opposé au "besoin d'en connaître"

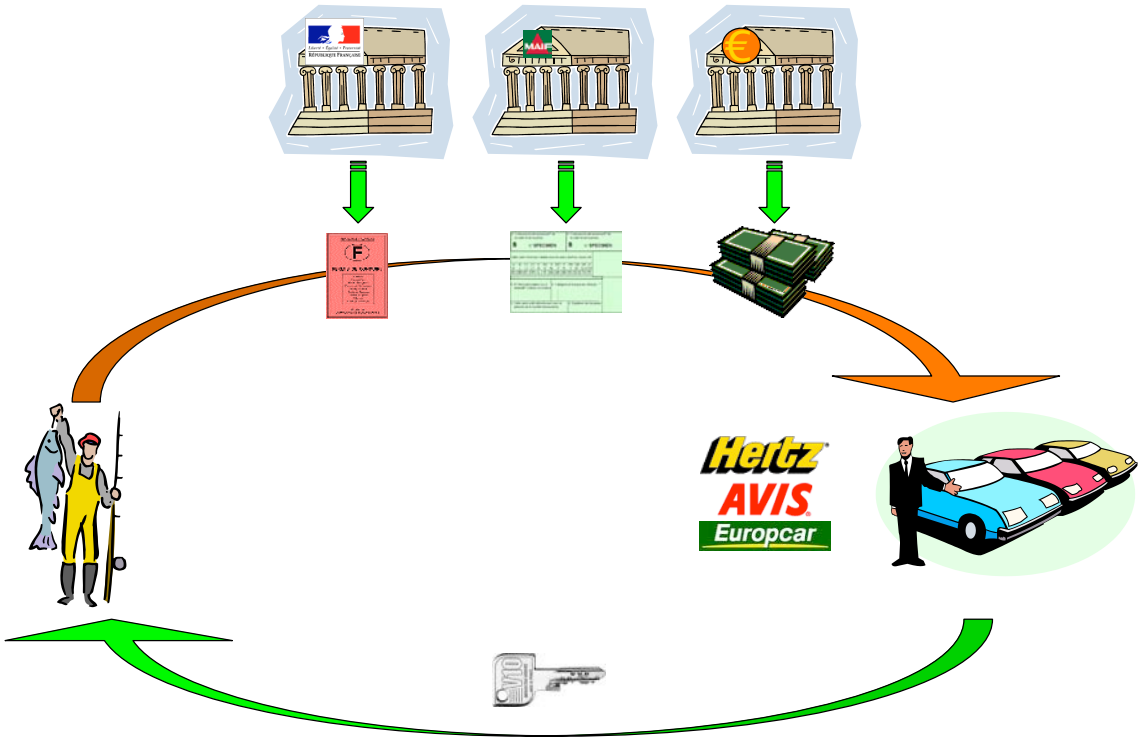
Preuves d'autorisation: credentials

- *Credential* = garantie, accréditation
- Exemples :
  - cartes d'abonnement, de membre d'association, …
  - permis de conduire, carte d'identité, d'électeur, …
- Certificats multiples :

  ex: SPKI : certificats d'attributs/d'autorisation
- Certificats restreints :
  - *"Partial Revelation of Certified Identity"* Fabrice Boudot, CARDIS 2000
- Exemple : Carte d'identité blanche

<http://www.identitesactives.net/?q=reve-d-identite-11-carte-d-identite-blanche>

"Anonymous Credentials" (Idemix)



Signature de groupe

- Une clé publique de vérification de signature, *n* clefs privées de génération de signature.
- Le responsable de groupe distribue les clefs privées aux membres du groupe.
- Pour prouver qu'on est membre du groupe (= possède une accréditation anonyme), on chiffre un message aléatoire, vérifiable, signé par le groupe.
- La vérification de la signature est une preuve d'appartenance, donc d'accréditation.
- Seul le responsable de groupe peut vérifier quel membre a signé.

e-Cash (1)

- Propriétés souhaitées :
  - Anonymat : un billet n'identifie pas la personne pour laquelle il a été émis
  - Impossibilité de fabriquer des faux
  - Impossibilité de dépenser deux fois
  - Transmissibilité : un billet peut être échangé entre personnes
  - Liquidité : un billet peut être divisé en petites coupures, ou agrégé en coupures supérieures

e-Cash (2) : signature aveugle (*blind sign.*)

- Alice génère un nombre aléatoire R, le multiplie par un facteur secret S, et l'envoie signé à sa banque: A->B: $[R*S, \text{valeur}]_A$
- La banque débite le compte d'Alice de la valeur, et renvoie le billet signé à Alice : B->A: $[R*S, \text{valeur}]_B$
- Alice "désaveugle" le billet $[R, \text{valeur}]_B$, et le dépense chez un marchand
- Le marchand transmet le billet à la banque : M->B: $[R, \text{valeur}]_B$
- La banque vérifie la signature, enregistre le billet comme dépensé, et crédite le compte du marchand de la valeur, et notifie le marchand, qui donne un reçu à Alice
- Si Alice (ou le marchand) essaye de redépenser le billet, la banque trouvera le billet dans la liste des billets dépensés

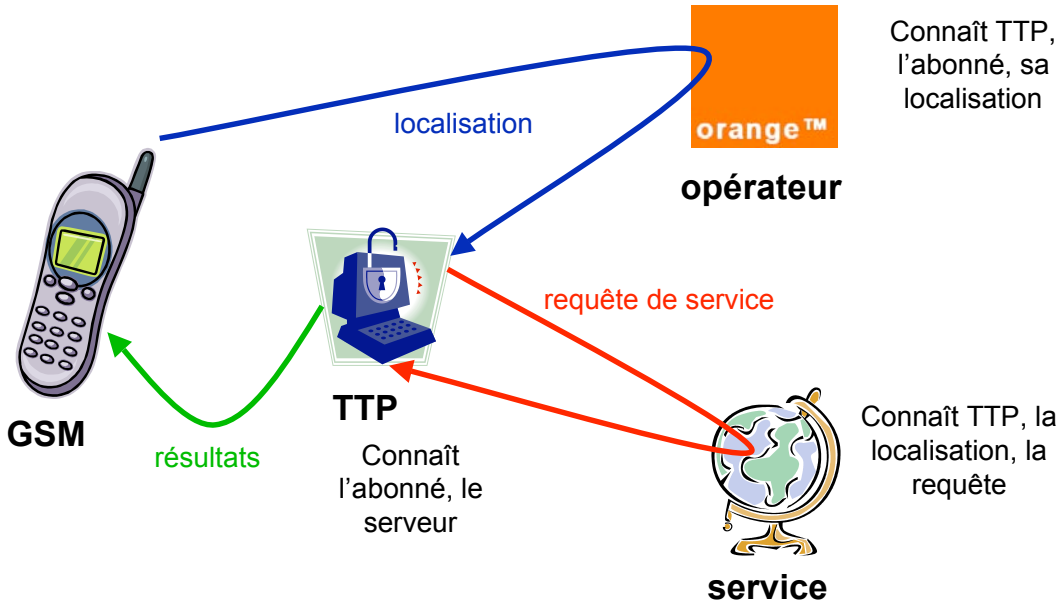
4° PET : gestion des données personnelles

- Négociation entre l'individu et l'entreprise
  "consentement éclairé"
  ex: coupons de réduction en échange d'une publicité ciblée
- Souveraineté : celui qui fournit des informations sur lui-même doit pouvoir contraindre l'usage qui pourrait en être fait --> Obligations
  ex: à effacer dans 48 h.
- Minimisation des données personnelles
  -> répartition : séparation des pouvoirs, fragmentation des données
  -> anonymisation + appauvrissement
  ex: remplacer le code postal par l'identifiant de la région

  -> Private Information Retrieval (PIR)

Service basé sur la localisation

- Ex: PRIME : pharmacie la + proche



4bis PET : Accès aux données

- Principe du moindre privilège : un individu ne doit avoir que les droits minimaux nécessaires à sa tâche
- Politique de sécurité et mécanismes de protection : le détenteur d'une information en est responsable (art 34 de la loi « informatique et libertés »)
- Ces données peuvent être très sensibles : ex: dossiers médicaux
  - Disponibilité : temps de réponse (urgence), pérennité
  - Intégrité : nécessaire à la confiance, éléments de preuve
  - Confidentialité : vie privée <-> intérêts économiques
- Privacy = contrôle d'accès + obligations

Donner confiance aux utilisateurs…

… que leur vie privée est protégée

- Certification & labellisation
- Approche Trusted Computing Group (TCG)
  - Support matériel : TPM
  - Bootstrap sûr
  - Vérification sceau S/W au chargement
  - Vérifiable à distance, sans dévoiler d'identité (DAA)

PRIME (03/2004 - 05/2008)

http://www.prime-project.eu/

- Privacy and Identity Management for Europe
  - Aspects juridico-socio-économiques
  - PET Côté utilisateur (dévelopt, utilisabilité)
  - PET Côté système, réseau, serveur
  - Applications réelles
- 20 Partenaires, 16 M€, subvention : ~10 M€
  - Fournisseurs (IBM, HP, …)
  - Labos (KUL, U. Dresde, U. Milan, LAAS…)
  - Utilisateurs (Lufthansa, T-Mobile, Swisscom, HSR)
- Final Event : 21 juillet 2008 à Leuven (B)

Conclusion

- Analyser les impacts sur la vie privée dès la conception de nouvelles technologies
- Respecter les principes de souveraineté et de minimisation des données personnelles
- Développer des nouveaux objets personnels pour faciliter la protection de la vie privée : ex. stockage de données personnelles, gestion des identités, e-Cash, *anonymous credentials*, carte d'identité blanche …

Bibliographie <mailto: deswarte@laas.fr>

- *Sécurité des systèmes d'information,* V.2, dir. Ludovic Mé & Yves Deswarte, Traité IC2, série Réseaux et télécommunications, Hermès, ISBN 2-7462-1259-5, 390 pp., juin 2006.
- Simone Fischer-Hübner, *IT-Security & Privacy*, LNCS 1958, Springer, 2001.
- Stefan A. Brands, *Rethinking Public Key Infrastructures and Digital Certificates*, MIT Press, 2000.
- Yves Deswarte, David Powell, Yves Roudier, « Sécurité, protection de la vie privée et disponibilité », chapitre XIII in *Informatique diffuse* (dir. V. Issarny), Arago 31, OFTA, Paris, mai 2007, ISBN 2-906028-17-7, pp. 301-344. <http://www.lavoisier.fr/notice/gb/not2.asp?id=36ONXOZ3SRLOFJ>
- Yves Deswarte, Carlos Aguilar-Melchor, "Current and Future Privacy Enhancing Technologies for the Internet", *Annales des Télécommunications*, vol.61, n°3-4, March/April 2006.
- Yves Deswarte, Carlos Aguilar-Melchor, Vincent Nicomette, Matthieu Roy, "Protection de la vie privée sur Internet", *Revue de l'Électricité et de l'Électronique* (*REE*), octobre 2006 (n°9), pp.65-74.
- Carlos Aguilar-Melchor, "Les communications anonymes à faible latence", Thèse de l'Institut National Polytechnique de Toulouse, 4 juillet 2006, LAAS n°06571.