Confiance et protection de la vie privée

Yves Deswarte
deswarte@laas.fr

LAAS-CNRS, Toulouse

Sécurité & protection de la vie privée

- "Privacy" ≈ confidentialité de données (et méta-données) personnelles
  PII : Personally Identifiable Information
- = sous-ensemble de "sécurité" (CIA)
- Mais…

… "*the devil is in the details*"

- Garder les justificatifs, en cas de litige
- Traçabilité des actions
- Authentification forte
- … danger pour la vie privée !!!

1er Principe pour protéger la vie privée :

- "Besoin d'en connaître" ("need-to-know")
  ne transmettre une information qu'à ceux qui en ont besoin pour réaliser la tâche qu'on leur confie
  -> Minimisation des données personnelles
  puis destruction/oubli
- … sur Internet 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

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 …

2ème Principe pour protéger la vie privée :

- "Auto-détermination" : 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…

PETs : Privacy-Enhancing Technologies

- Protéger les adresses IP : MIX…
- Gestion d'identités multiples
  - Accès anonyme à des services
  - Autorisation respectant la vie privée
- Gestion des données personnelles

Gestion d'identités multiples

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

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)

Autorisation sur Internet

- Aujourd'hui : 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 compatibilité entre les politiques de sécurité/privacy "déclarées"

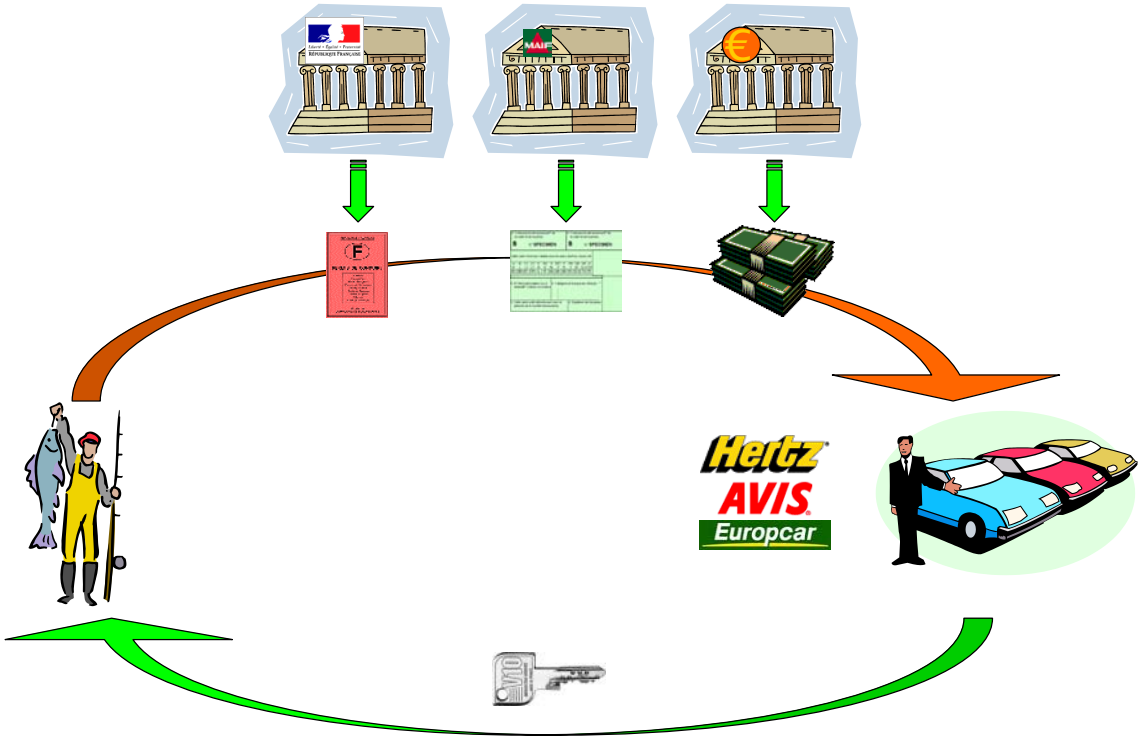
Ce schéma est dépassé

- 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

- Certificats multiples :
  ex: SPKI : certificats d'attributs/d'autorisation
  - cartes d'abonnement, de membre d'association, …
  - permis de conduire, carte d'électeur…
- Problèmes: "chaînabilité" (une seule clé publique pour plusieurs certificats?), gestion des certificats/clés, authentification, préservation des preuves, révocation, …
- Certificats restreints :
  - "Partial Revelation of Certified Identity"
    Fabrice Boudot, CARDIS 2000

"Anonymous Credentials" (Idemix)



Gestion des données personnelles

- Négociation entre l'individu et l'entreprise
  ex: coupons de réduction en échange d'une publicité ciblée
- Auto-détermination : 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)

Accès aux données personnelles

- 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 critiques :
  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 leurs données personnelles sont bien protégées ?

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

Protection des données personnelles…

… même contre des personnes malveillantes ?

- Contrôle d'accès renforcés, contrôle de flux (y compris contre des utilisateurs privilégiés)
- Obligations "incontournables"
- Chiffrement : Identity-based encryption, policy-based encryption, sticky policies, …
- Tolérance aux intrusions (ex. fragmentation-dissémination)

PRIME (03/2004 - 02/2008)

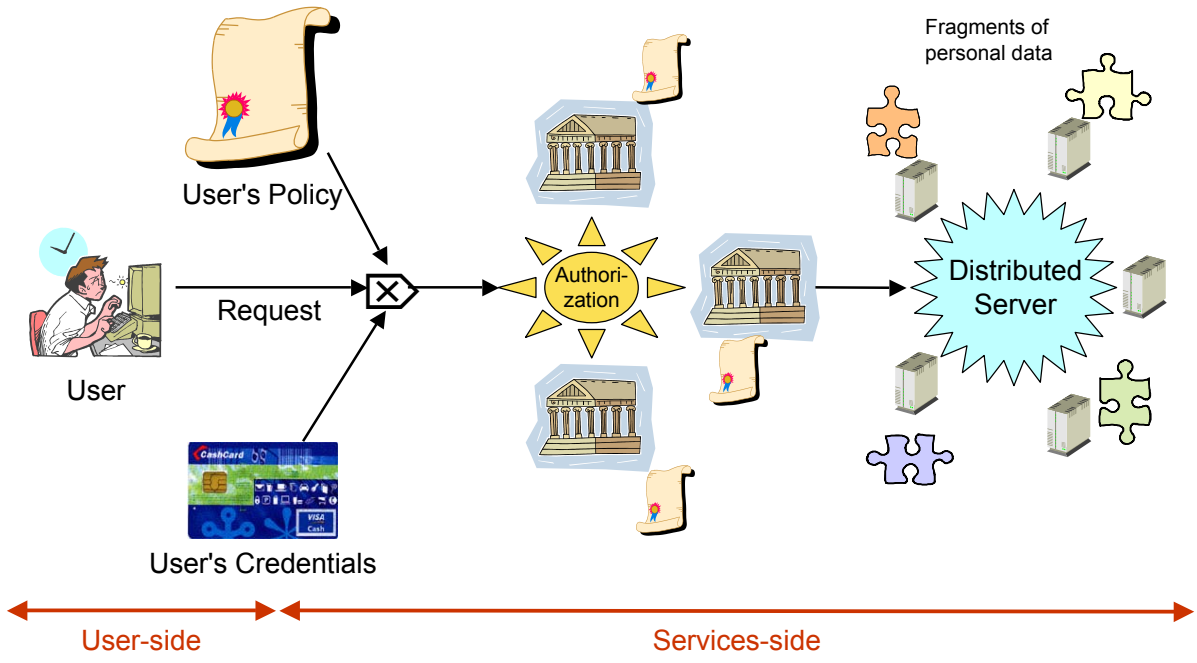
http://www.prime-project.eu.org/

- 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, Eurécom, LAAS…)
  - Utilisateurs (Lufthansa, T-Mobile, Swisscom, HSR)

PRIME Principe :

- Identités différentes selon les besoins

Exemple d'architecture



Trust Management (HP Bristol)

- Vérification capacités plateforme : TPM
- Vérification label (procédures, audit)
- Vérification du respect des obligations
  - Test par TTP
  - Mécanismes de réputation

Bibliographie

- Simone Fischer-Hübner, *IT-Security & Privacy*, LNCS 1958, Springer, 2001.
- Stefan A. Brands, *Rethinking Public Key Infrastructures and Digital Certificates*, MIT Press, 2000.
- *Sécurité des systèmes d'information V.2*, dir. Ludovic Mé & Yves Deswarte, Traité IC2, série Réseaux et télécommunications, Hermès, ISBN 2-7462-1259-5, 372 pp., juin 2006.
  <http://www.lavoisier.fr/fr/livres/index.asp?texte=2746212590&select=isbn&from=Hermes>
- Yves Deswarte, Carlos Aguilar-Melchor, "Current and Future Privacy Enhancing Technologies for the Internet", *Annales des Télécommunications*, vol. 61 n° 3-4, mars-avril 2006, pp. 399-417.
- Yves Deswarte, Carlos Aguilar-Melchor, Vincent Nicomette, Matthieu Roy, "Protection de la vie privée sur Internet", à paraître dans *Revue de l'Électricité et de l'Électronique (REE)*, 2006.