Privacy-Enhanced Ambient Intelligence

Yves Deswarte
deswarte@laas.fr

LAAS-CNRS, Toulouse

Ambient Intelligence

- New technologies are being developed: useful or practical devices/services

- Market created/developed by technology providers: hardware, networks, services, …

- … but most often without privacy concern

Example: RFID

- Unique identifier for each object,
  readable without visibility
- Better supply management, stock management,
  traceability for containers/contents,
  food safety, customer support, …
- But possibility of customer tracing
- … danger for privacy !!!

Outlines

- *Privacy* : Definitions
- Basic Principles
- PETs : Privacy Enhancing Technologies
  - Managing Multiple Identities
  - Anonymous Communications and Accesses
  - Privacy-Preserving Authorization
  - Personal Data Management

Privacy: definitions

- *"The state or condition of being free from being observed or disturbed by other people"*

- Common Criteria (CC V3.1, also ISO 15408) :
  Privacy = one functional class, with 4 requirements
  to provide a user protection against discovery and misuse of identity by other users :
  - Anonymity: ensures that a user may use a resource or service without disclosing the user's identity
  - Pseudonymity: ensures that a user may use a resource or service without disclosing its user identity, but can still be accountable for that use
  - Unlinkability: ensures that a user may make multiple uses of resources or services without others being able to link these uses together
  - Unobservability: ensures that a user may use a resource or service without others, especially third parties, being able to observe that the resource or service is being used

Pseudonymity < anonymity < unlinkability < unobservability

Basic Principles

1st Principle to protect privacy:

- "Sovereignty": the person shall maintain control on his/her personal [meta-]data

  -> stored on a personal device:
  (smartcard, PDA, PC…)

  -> if these data are disclosed to a third party, impose **obligations** on their use

  - Expiration dates
  - Notification in case of transfer or unexpected use
  - etc…

- Example: Application to Sensor Networks: transmit personal data only to personal devices

2nd Principle to protect privacy:

- Personal Data Minimization
  personal information shall be transmitted only to those who need it to achieve the task they have been entrusted with -> "*need-to-know*"
  then destroy/forget

- … on the Internet like in the real world

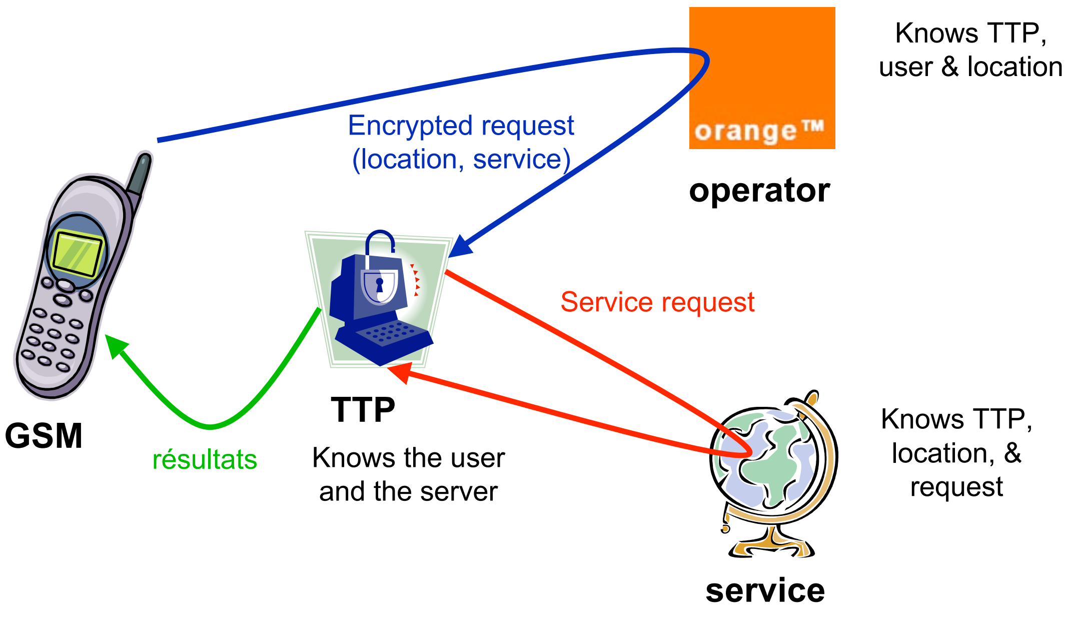
- … with limits: some personal data must be provided to judiciary authorities in case of dispute or investigation (e.g., against money laundering) : pseudonymity rather than total anonymity

Links: minimization <--> proportionality and legitimate purpose

Ex: Which information may be transmitted by a RFID?

Example of location-based service

- Ex: PRIME : the closest pharmacy



Privacy-Enhancing Technologies

PETs : *Privacy-Enhancing Technologies*

- Managing Multiple Identities
- Anonymous Communications and Accesses
- Privacy-Preserving Authorization
- Managing Personal Data

1st PET: Managing Multiple Identities

- Identity = the representation of a physical person
- Reduce/control the links between the person and the personal data (and meta-data): control the *linkability*
  - communications and accesses are supposed to be unlinkable
- But: customized/privileged accesses: virtual identity = pseudonym
  - Preferences (ex: meteo) -> "*cookies*"
  - Different roles -> different pseudonyms
    - Ex: tax payer and elector
  - Authentication strength should be adapted to the risks of identity theft (and liablity)
  - Lifetime should be adapted to the needs of linkability
    -> throw-away pseudonyms
- Multiple virtual identities vs. "*single-sign-on*"
  Liberty Alliance <http://www.projectliberty.org>
  vs. Microsoft Passport

IP@ identifying data

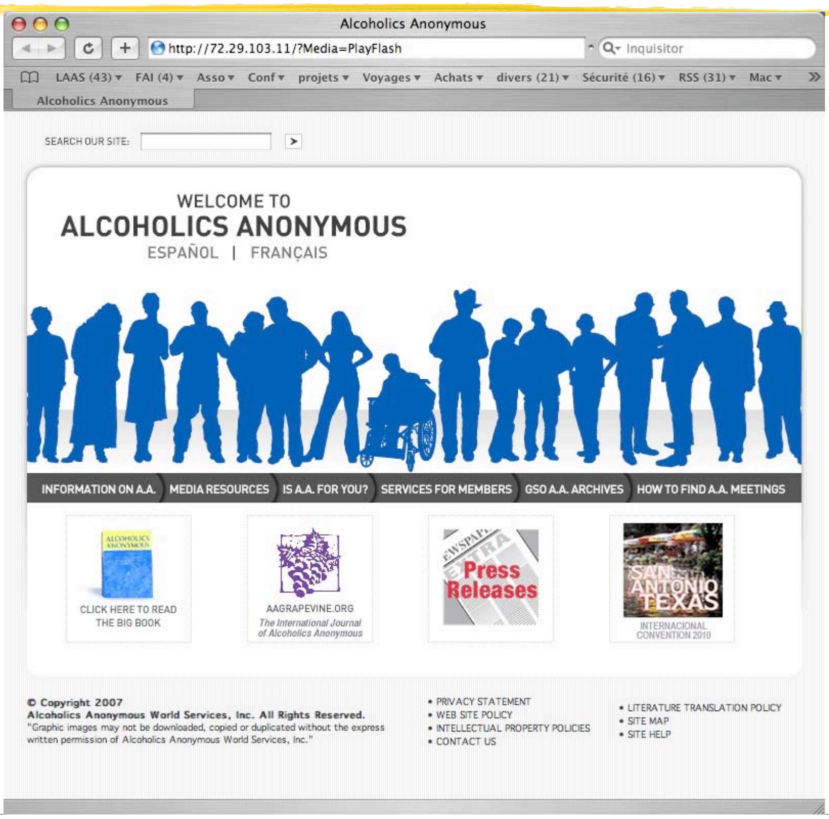
Example :

```
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] (messiaen [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
```

IP@ = sensitive content

Example :

http://72.29.103.11/


Alcoholics Anonymous

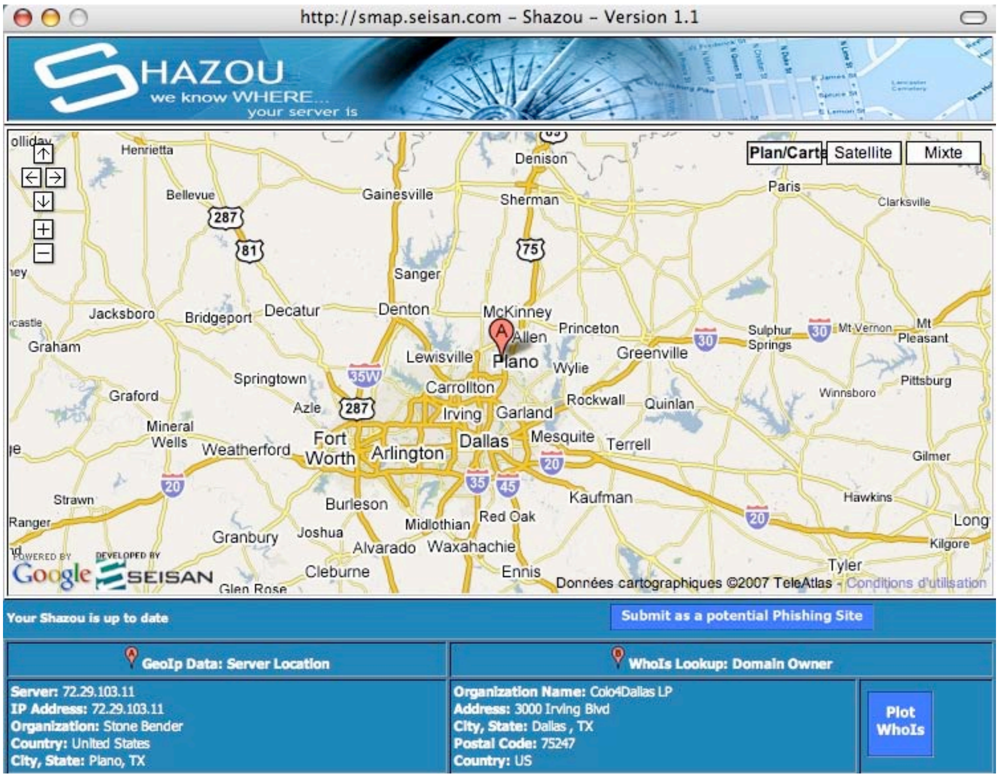
http://72.29.103.11/?Media=PlayFlash

WELCOME TO
ALCOHOLICS ANONYMOUS
ESPAÑOL | FRANÇAIS

© Copyright 2007
Alcoholics Anonymous World Services, Inc. All Rights Reserved.
"Graphic images may not be downloaded, copied or duplicated without the express written permission of Alcoholics Anonymous World Services, Inc."

IP@ = location information

Example :



http://smap.seisan.com – Shazou – Version 1.1

SHAZOU we know WHERE... your server is

Your Shazou is up to date

Submit as a potential Phishing Site

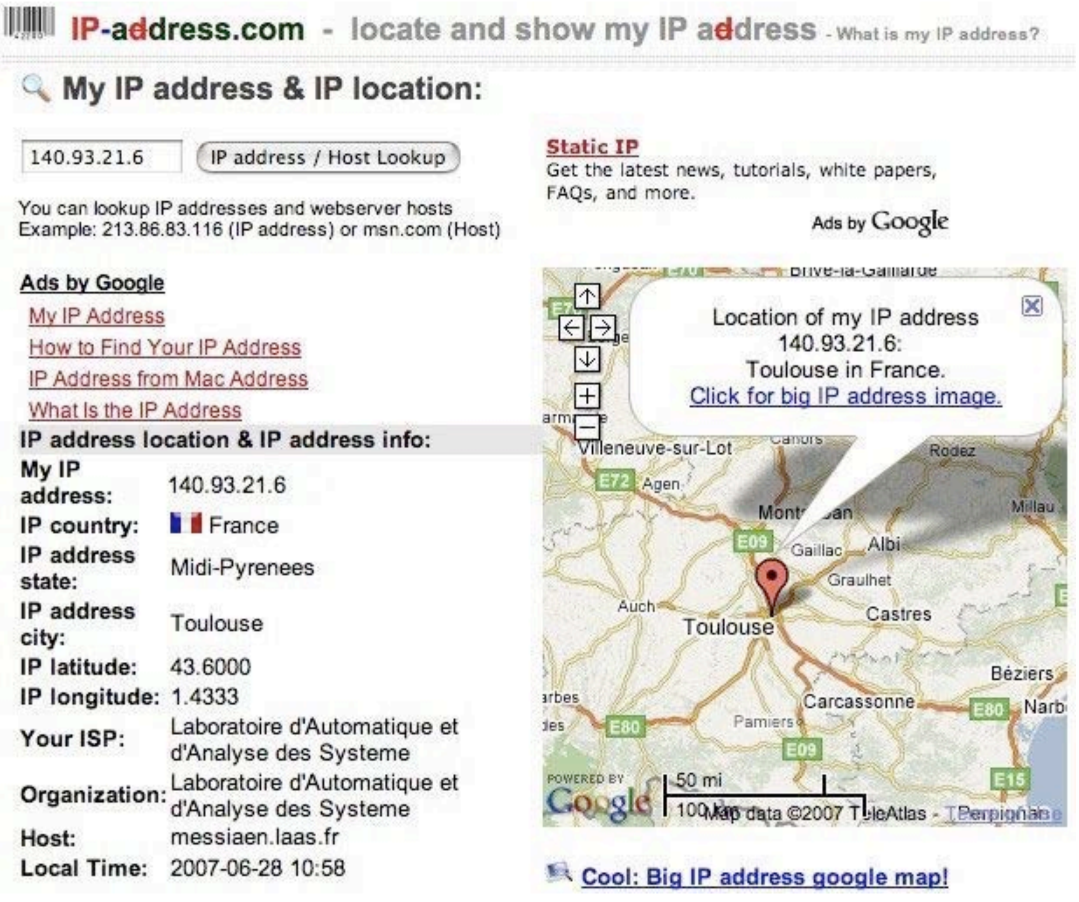
GeoIp Data: Server Location

Server: 72.29.103.11
IP Address: 72.29.103.11
Organization: Stone Bender
Country: United States
City, State: Plano, TX

WhoIs Lookup: Domain Owner

Organization Name: Colo4Dallas LP
Address: 3000 Irving Blvd
City, State: Dallas , TX
Postal Code: 75247
Country: US

Plot WhoIs



IP-address.com - locate and show my IP address - What is my IP address?

My IP address & IP location:

140.93.21.6 | IP address / Host Lookup

You can lookup IP addresses and webserver hosts
Example: 213.86.83.116 (IP address) or msn.com (Host)

Ads by Google
- My IP Address
- How to Find Your IP Address
- IP Address from Mac Address
- What Is the IP Address

Static IP
Get the latest news, tutorials, white papers, FAQs, and more.

Ads by Google

IP address location & IP address info:

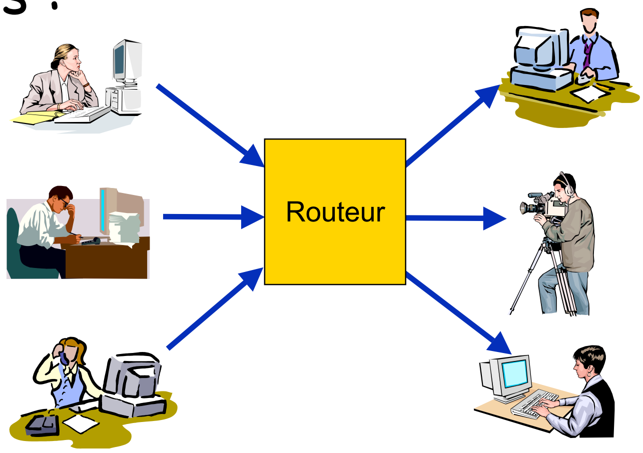
My IP address:	140.93.21.6
IP country:	France
IP address state:	Midi-Pyrenees
IP address city:	Toulouse
IP latitude:	43.6000
IP longitude:	1.4333
Your ISP:	Laboratoire d'Automatique et d'Analyse des Systeme
Organization:	Laboratoire d'Automatique et d'Analyse des Systeme
Host:	messiaen.laas.fr
Local Time:	2007-06-28 10:58

Location of my IP address 140.93.21.6: Toulouse in France.
Click for big IP address image.

Cool: Big IP address google map!

2nd PET: Anonymous Communications

- To protect IP@:
  dynamic assignment of IP addresses:
  (DHCP, PPP, NAT, …)
- Anonymity routers :
  - MIX
  - Onion Routing
  - Crowds



IP V6, ad hoc networks, …

- Tomorrow : IP everywhere (*pervasive/ubiquitous computing, ambiant intelligence, sensor networks, RFID, 4G convergence …*)
- every device will have an implicit IP@ *unique and permanent* (based on a manufacturing serial number)
- Every person will own several devices …
- … that will connect to other close devices (ad hoc)
- … that will identify each other, route their communications, provide contextual information, etc.

Anonymous IP roaming connection

Roaming : Laptop, PDA, mobile phone …

1. Generate a random MAC@
2. Obtain a temporary IP@
3. Tunnel towards a roaming TTP
4. Generate another IP@
5. ISP authentication

3th PET: Privacy-Preserving Authorization

- Today: client-server
  the server grants or denies access/privileges to the client accorded to its claimed identity (possibly verified with authentication mechanisms)
- The server must record personal data:
  to serve as evidence in case of dispute
- These data may be used for other purposes (customer profiling, direct marketing, customer file trading, black-mailing…)
- Action P3P (W3C) : *Platform for Privacy Preferences Project*
  automatic verification of claimed security/privacy policies

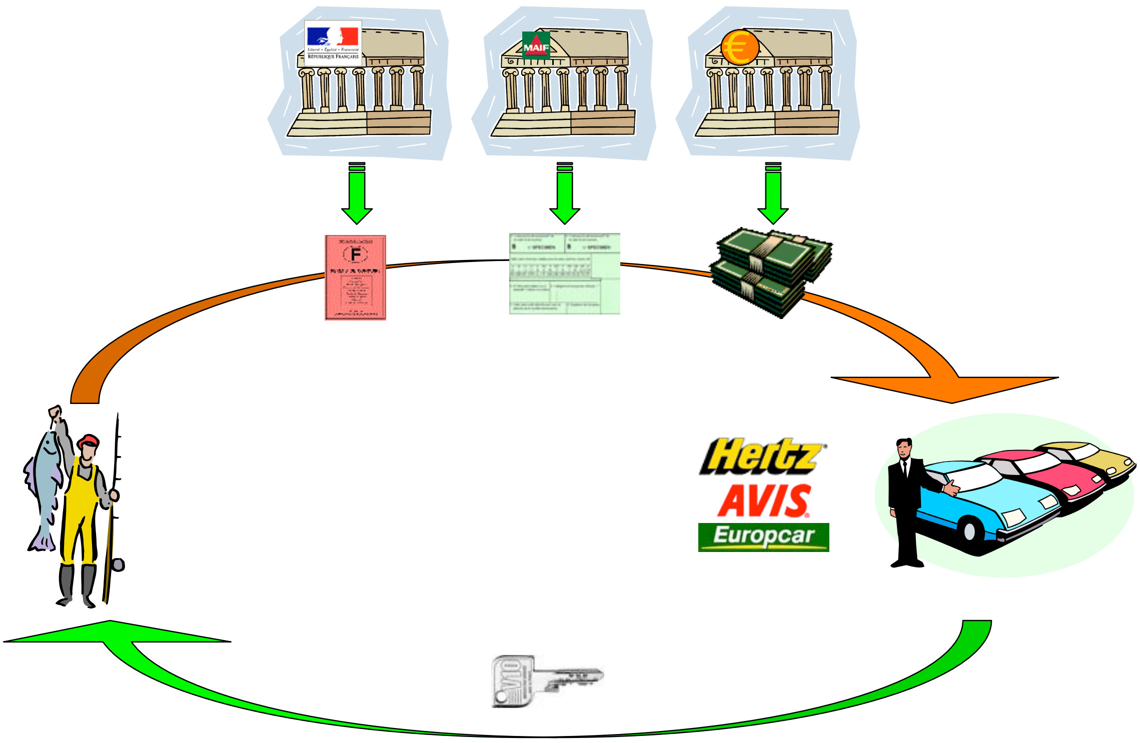
This scheme is obsolete!

- Internet transactions involve generally more than 2 parties
  (ex : electronic commerce)
- These parties have different (or even opposed) interests: mutual suspicion
- Privacy intrusive:
  contrary to need-to-know principle

Authorization Proofs: Credentials

- Multiple Certificates:
  ex: SPKI : attribute/authorization certificates
  - Subscription cards, association member cards, …
  - Driver's license, elector's card, identity card, …
- Problems: linkability (can you trust the CA?, one single public key for several certificates?), managing certificates/keys, authentication, collecting evidence, revocation, …
- Restricted Certificates:
  - "Partial Revelation of Certified Identity"
    Fabrice Boudot, CARDIS 2000

Anonymous Credentials (Idemix)



Group Signature

- One single public verification key, *n* private signature keys.
- The group manager distributes a different private key to each group member.
- To prove group membership (i.e., ownership of an anonymous credential), sign a random message that is verifiable with the group verification key.
- Signature verification is a proof of membership, i.e. of credential ownership.
- Only the group manager can recognize who has signed a message.

4th PET: Managing Personal Data (1)

- Sovereignty: the personal data owner (i.e., the person) can impose constraints on the data use
  --> Obligations
  ex: to be deleted in 48 h.
- Minimization of personal data
  -> distribution: separation of duty,
  data fragmentation
  -> anonymization + obfuscation
  ex: remplace zip code by region identifier

  -> Private Information Retrieval (PIR)

4th PET: Managing Personal Data (2)

- Least Privilege Principle: any individual should have the minimal rights necessary for the assigned task
- Security Policy and Protection Mechanisms: the personal data keeper is responsible for them
- These data may be very critical:
  ex: patient medical records
  - Availability: response time (emergency), long time storage
  - Integrity : needed for trust, evidence
  - Confidentiality : privacy <-> economic interests
- Privacy = access control + obligations

Conclusions

- Analyze impacts on privacy when designing new technologies

- Obey the principles of personal data *sovereignty* and *minimization*

- *Develop new personal devices to enhance privacy* : personal data storage, identity management, anonymous credentials, e-Cash, …

Bibliography

- 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>

- *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, 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.