



Laboratoire d'Informatique de Grenoble – LIG  
Équipe STEAMER



# Mécanismes de sécurité et de respect de la vie privée adaptés au contexte dans les systèmes pervasifs

**José Bringel Filho\***

[Jose.de-Ribamar-Martins-Bringel-Filho@imag.fr](mailto:Jose.de-Ribamar-Martins-Bringel-Filho@imag.fr)

**Hervé MARTIN**

Directeur de thèse

\* Thèse financée par Alban (UE)



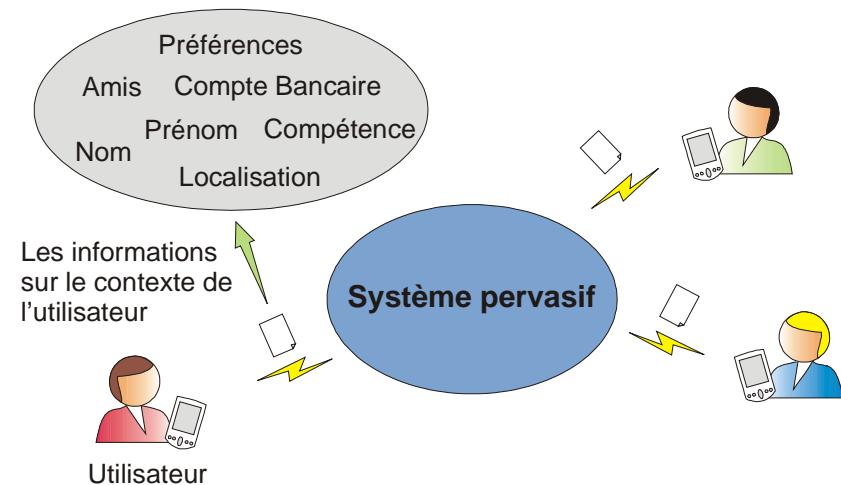
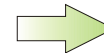
**GT Services Localisés**  
Jeudi 25 oct 2007, Paris

# Environnements Computationnels Pervasifs (PCE) sensibles au contexte

- **Adapter les fonctionnalités du système à chaque utilisateur**
  - identifier le contexte de l'utilisateur lors de l'accès au système
  - accéder à l'ensemble des préférences et des attributs de l'utilisateur



**Accéder aux informations personnelles confidentielles**  
(préférences, historique d'utilisation des services)



## Risques de sécurité

- La confidentialité
- L'intégrité
- La vie privée

# Les requis de sécurité dans les PCE

- **Être anonyme (anonymity)**
  - l'identité réelle d'un utilisateur ne doit pas être révélée pendant la communication avec les fournisseurs de services sans que celle-ci ait été intentionnellement divulguée par l'utilisateur
- **La vie privée du contexte**
  - Aucun service ou autre utilisateur ne doit être capable d'obtenir des informations contextuelles d'un utilisateur avec précision
    - la localisation, la durée, le type de requête au service
- **La confidentialité et l'intégrité**
  - l'interaction entre un utilisateur et un service ainsi que les données résultantes doivent respecter les niveaux de confidentialité et la vie privée défini par l'utilisateur
    - la protection de la communication, des données personnels

# Principaux défis de la vie privée et la sécurité dans les PCE

- **Les défis sont liés aux aspects de :**
  - la non intrusivité d'environnement
  - la localisation d'utilisateur
  - la sensibilité au contexte
  - la quantité de données capturée
  - fournisseurs de services
  - l'absence de propriété des ressources

# Principaux défis de la vie privée et la sécurité dans les PCE

- **La non intrusivité d'environnement**

- les technologies doivent être embarquées en minuscules dispositifs capables de communiquer entre eux et d'interagir avec les environnements
  - ✚ réduit la visibilité et la perception de l'utilisateur par rapport à l'environnement, mais le rend plus acceptable
  - ✖ permet à l'environnement d'envahir facilement la vie privée de l'utilisateur
  - ✖ réduit le contrôle de l'utilisateur sur la vie privée et lui ajoute la responsabilité de respecter la vie privée des autres

# Principaux défis de la vie privée et la sécurité dans les PCE

- **La localisation d'utilisateur**

- les SP ont pour habitude d'utiliser des informations de localisation de l'utilisateur afin de fournir des services adaptés
  - ✚ utiliser la localisation exacte de l'utilisateur ou déduire une relation de proximité pour s'adapter à leur comportement
    - services de trafic, de cartes de navigation, de localisation des restaurants proches à l'utilisateur
  - ▣ la grande majorité des personnes ne perçoivent pas toute implication à révéler leur localisation, excepté dans quelques situations
    - localiser la population judaïque (seconde guerre mondiale)
- la protection des informations de localisation doit être adaptée au contexte
  - permettre la divulgation de ces données est souhaitable dans quelques situations
    - situation d'urgence

# Principaux défis de la vie privée et la sécurité dans les PCE

- **La sensibilité au contexte**
  - ✚ fournir des services adaptés au contexte sans révéler l'identité de l'utilisateur
  - ▣ chacune de ces informations possède des restrictions de sécurité différentes qui sont liés à la sensibilité et aux préférences de l'utilisateur
  - ▣ chaque utilisateur désire contrôler précisément les services et les données qui seront partagés et dans quel contexte
    - Quelles sont les ressources que je désire partager ? Avec qui? Et dans quel contexte?

# Principaux défis de la vie privée et la sécurité dans les PCE

- **La quantité de données capturée**
  - l'implémentation des PCE compte avec l'augmentation de la quantité et de la qualité des données capturés et produites dans l'environnement
    - ✚ permettre l'adaptation par rapport plusieurs aspect et dimensions contextuelles
    - ▣ les préférences des utilisateurs sont fréquemment ignorées par rapport à la vie privée sur ces données
    - ▣ un service seulement devrait avoir accès aux informations sur le contexte de l'utilisateur susceptibles d'être exploitées lors de son exécution
      - « Principe de la réduction au minimum des données » défini par le Parlement et le Conseil Européen (Directive 2002/58/EC)

# Principaux défis de la vie privée et la sécurité dans les PCE

- **Fournisseurs de services**
  - Les services fournis peuvent être liés au travail ou à la vie personnelle des utilisateurs
    - ✚ fournir des services aux utilisateurs adaptés à leurs nécessités de manière réactive ou proactive
    - ✖ les informations contextuelles peuvent révéler le comportement personnel des utilisateurs
      - leurs habitudes, leurs préférences, leurs aversions et leurs associations
    - ✖ l'utilisation abusive des informations personnelles par un fournisseur intrus

# Principaux défis de la vie privée et la sécurité dans les PCE

- **L'absence de propriété des ressources**
  - Continuellement l'environnement perd la liaison existante entre les propriétaires et les ressources
    - ✚ L'environnement plus dynamique
    - ✚ L'implémentation du contrôle d'accès à des ressources est complexe quand le propriétaire ne peut pas être facilement déterminé
      - Par exemple, sur une caméra de sécurité d'une bâtiment

# Les mécanismes de sécurité dans les PCE

- **Doivent être incorporés aux environnements**
  - protéger la communication, les données résultant des interactions avec les utilisateurs, les informations contextuelles
- **Doivent être présents dans les dispositifs mobiles participant**
  - contrôler l'accès aux ressources locales des utilisateurs
- **Doivent être adaptés à les informations contextuelles**
  - par exemple, prendre en compte les dimensions spatio-temporels et computationnels

# L'objectif

**« Appliquer, de façon adaptée au contexte, les mécanismes de sécurité et les politiques par rapport à la vie privée pour la protection de la communication et des données résultant des interactions entre les utilisateurs et l'environnement, ainsi que les informations contextuelles »**

# Conclusion

- **Une grande partie des recherches sont focalisées sur les problèmes de la vie privée par rapport à les informations de localisation de l'utilisateur**
  - Comment fournir des services adapté à les informations de localisation et au même temps d'éviter sa diffusion à toute les autres entités ?
- **Les recherches relatives à la perception de contexte et à la quantité de données capturées n'ont pas été intensifiées**
  - Un des objectifs de ce travail

# La solution envisagée

- **Proposer une solution de gestion d'informations contextuelles**
  - Permettre d'écrire des contextes spatio-temporels et computationnels qui seront évalués par le système afin d'appliquer les mécanismes de sécurité adaptés à la situation
    - à l'intérieur de ma salle de travail, entre 8h et 18h, pendant la semaine
    - dans la salle d'attente de l'aéroport
- **L'addition de mécanismes de sécurité dans la couche d'application**
  - Fournir les services de la confidentialité, de l'intégrité et de la vie privée adapté au contexte spatio-temporels et computationnels
    - En utilisent le FRAMESEC et l'outil PEARL
  - Protection des informations contextuelles en utilisent des politiques de sécurité
  - Indépendance des technologies de communication sans fil (e.g., wifi, bluetooth) et du capteur d'informations de localisation utilisée (e.g., GPS, Active Bagdes)

# Les travaux futurs

- **Travaux futurs**

- Proposer une extension aux modèles de contexte existants
  - Prendre en compte le respect à la vie privée d'utilisateur
  - Des ontologies OWL pour la représentation
- Proposer une architecture capable d'identifier les contextes spatio-temporel et computationnel actuels afin d'appliquer les mécanismes de sécurité conforme aux politiques décrites par les utilisateurs
  - suis-je dans l'immeuble où je travaille ? Dans ma salle ? À la maison ?  
Quelles politiques de sécurité appliquées dans un certain contexte ?

# Références

- Ren, K.; Lou, W.; Deng, R.; Kim, K. A novel privacy preserving authentication and access control scheme in pervasive computing environments. *IEEE Trans Veh Technol* 55(4):1373-1384, July (2006).
- Ren, K. and Lou, W. 2007. Privacy-enhanced, attack-resilient access control in pervasive computing environments with optional context authentication capability. *Mob. Netw. Appl.* 12, 1 (Jan. 2007), 79-92.
- Bhaskar, P. and Ahamed, S. I. 2007. Privacy in Pervasive Computing and Open Issues. In *Proceedings of the the Second international Conference on Availability, Reliability and Security* (April 10 - 13, 2007). ARES. IEEE Computer Society, Washington, DC, 147-154.
- Cas, J., Privacy in pervasive computing environments - a contradiction in terms?, *Technology and Society Magazine*, IEEE, Volume 24, Issue 1, Spring 2005, pp. 24-33
- Henricksen, K., Wishart, R., McFadden, T., Indulska, J., Extending context models for privacy in pervasive computing environments, *Third IEEE International Conference on Pervasive Computing and Communications Workshops*, 8-12 March 2005 pp.20-24
- Pigeot, C., Gripay, Y., Scaturici, M., Pierson, J. Context-Sensitive Security Framework for Pervasive Environments. Dans : *European Conference on Universal Multiservice Networks (ECUMN 2007)*, Toulouse, 14/02/07-16/02/07, IEEE Computer Society, p. 391-400, février 2007