PRIAM

Privacy Issues in AMbient intelligence

Kickoff Meeting Report

25/01/2007

INSTITUT NATIONAL
DE RECHERCHE
EN INFORMATIQUE
ET EN AUTOMATIQUE

INRIA
RHÔNE-ALPES

Plan

1. Partners

- Background wrt PRIAM
- Potential contributions to PRIAM
- Expectations from the project

2. Precise definition of the scope of the project

- Technologies (devices, communication means, etc.)
- Types of personal data and case studies
- Legal framework

3. Objectives and approaches

- WP1: legal issues
- WP2 : privacy policies, modelization
- WP3 : implementation (feasibility study): OS, communications, cryptography

Part 1. Partners

- Inria – POPART
- Inria – Aces
- Inria – Ares
- University Jean Monnet
- University of Twente

Inria – POP-ART

Participants

- Daniel Le Métayer : modelization, verification, security, legal issues

- Nathalie Descot (post-doc): legal issues

Potential contributions

- WP1: status of existing regulations, new problems posed by the AI context, requirements/proposals for adaptations of the regulations

- WP2: formal definition of privacy policies which are :

    - consistent with the regulations (possibly adapted as put forward in WP1)
    - suitable in the AI context (user acceptance and effective implementation)

Inria – ACES

Participants

- Ciaran Bryce : OS, Java environments, security, DRM, TPM

- Potential post-doc

- PhD student: RFID technologies

Potential contributions

- WP3: secure communications

- WP3: access control, data protection, use of TPM technology

- WP3: secure logs

Inria – ARES

Participants

- Stéphane Ubéda : ad-hoc and hybrid networks, trust management

- Frédéric Le Mouël: trust management, e-home services, gateways

- Marine Minier: cryptography (algorithms, protocols), trust management

Potential contributions

- WP3: authentication techniques, secure communications

- WP3: trust management

- WP3: negotiation of privacy policies ?

- WP3: secure services

University Jean Monnet

Participants

- Joël Moret-Bailly : technology and law, deontology

Potential contributions

- WP1: legal issues
- WP4 : dissemination, contacts with lawyers

University of Twente

Participants

- Sandro Etalle : DRM, privacy policy models, a posteriori enforcement, collaborative environments

- M.A.C Dekker: privacy policy models, a posteriori enforcement

Potential contributions

- WP2: privacy policy models and logics

Part 2: Scope of the project

Terminology:

Ambient intelligence = ubiquitous computing + ubiquitous communications + intelligent user interfaces

Pervasive systems = ubiquitous computing

Spontaneous information systems = spontaneous establishment of communications among unknown devices

Self-organized networks = self-configuration, administration and repairing of networks (self-allocation of IP addresses, routing, etc.)

Ad-hoc networks = networks without any central and static communication infrastructure

Peer-to-peer : three interpretations:

- Architecture level : P2P architecture = no distinguished role (as opposed to client server e.g.)

- Application level: e.g. P2P content sharing applications

- Social level: model of community organization

Scope of the project : technologies

Devices

- Sensors
- Actuators
- RFID tags
- Cellular phones, PDA’s
- Gateways
- Personal Computers, laptops
- Trusted computing devices (TPM)
- Servers

Distinctive features relevant to PRIAM :

memory size, computation power, communication facilities, battery/batteryless

Scope of the project : Technologies

Networks, communication protocols

- Cellular networks (GSM, GPRS, UMTS)
- WLAN: WiFi, Wimax
- WPAN: Bluetooth
- Ad-hoc networks
- Internet, “Internet of things”

Distinctive features relevant to PRIAM :

central control/decentralized, dynamic/static, throughput, latency, communication range

PRIAM position

PRIAM will consider essentially hybrid networks (no restrictions or assumptions in terms of devices and/or networks)

Scope of the project : Case studies

Favorite case studies for PRIAM:

- Health care (medical information, active sensors for health monitoring, emergency situations, localization, etc.)
- Home environment (access to multimedia services, refrigerator, Internet, etc.)
- Ubiquitous commerce (supermarket, home, on the move, service delivery, etc.)

Other scenarios:

- Commercial services based on localization information
- Personalized commercial services
- Professional environment (professional card exchanges, address lists, etc.)
- Transportation, access control (train, airport, highway, company premises, etc.)
- E-Passport, identity card
- Internet of things, …

Distinctive features relevant to PRIAM : localization/no localization, private vs public place, level of sensitivity of the information, internet connection

Scope of the project : Personal information

Different types of personal information:

- Administrative
- Biological
- Behavioral
- Medical
- Localization
- Multimedia

Distinctive features relevant to PRIAM : sensitivity level, risk of data aggregation

Scope of the project : Regulation

National/regional regulations and case-laws:

- French law
- European directives (European Union)
- European Court of Human Rights (Council of Europe)

Private/business privacy policies ?

Most striking features of AI w.r.t. privacy

Features of AI which make things really different from already deployed technologies (Internet, cellular phones, smart cards, loyalty cards, etc.) w.r.t. privacy :

1. Mobility (dynamic federation of “microdomains”)
2. Pervasiveness (scale factor w.r.t. (1))
3. Lack of central control (connection of heterogeneous devices without any distinguished role, peer to peer architectures)

Part 3. Objectives and approaches

- WP1: legal and social issues
- WP2 : definition of privacy policies
- WP3 : implementation of privacy policies
- WP4: dissemination

Objectives and approaches
WP 1: legal and social issues

Objective 1 : state of the art

- Clear picture of existing regulations w.r.t. privacy (France, Europe, USA):

    - commonalities and differences among regulations
    - actual enforcement of the regulations

-Legal proofs (rules and practices w.r.t. electronic data)

Objectives and approaches
WP 1: legal and social issues

Objective 2: assess the suitability of current regulations w.r.t. the ambient intelligence context

- Do existing regulations provide appropriate protections ?

- Can they be implemented effectively ?

  - Technical feasibility (consent, purpose, access, modification, deletion, etc.)
  - User acceptance

Objectives and approaches
WP 2: definition of privacy policies

Requested (and challenging !) features

- Conditional rights (read, use, etc.) and obligations (owner information, consent request, deletion, etc.)

- Purpose (statistics, patient health care, etc.)

- Transfer (of rights and obligations)

- Revocation (of rights and obligations)

- Time (before/after, at occurrence of specific events, at specific time(s), etc.)

- Specific rights of the owner of personal data (access, modification, deletion, etc.)

Objectives and approaches
WP 2: definition of privacy policies

Desirable (and challenging !) features

- Notion of data aggregation
- Notion of liability / accountability
- Notion of trust (=> trade-offs, proportionality)
- Notion of data sensitivity (=> trade-offs, proportionality)
- Options (parameterized policies)

Objectives and approaches
WP 2: definition of privacy policies

Privacy policy model

- Non ambiguous (formal) semantics

- Decision algorithm to check the validity of actions (a priori / a posteriori)

- Comparison (or refinement) of security policies

- Composition of security policies

- Evolution of security policies (over time, through a negotiation process) ?

- User understanding (natural language or P3P-style translation ?)

Objectives and approaches
WP 3: implementation of privacy policies

Range of techniques :

- Identification / authentication : Inria-ARES + Inria-ACES
- Trust management : Inria-ARES
- Privacy policy agreement / negotiation : Inria-POPART + Inria-ARES ?
- (Secure) communication (secure channel): Inria-ARES + Inria-ACES
- Anonymisation : Inria-ARES
- Access control / data protection (DRM-like) : Inria-ACES
- Secure log : Inria-ACES

Objectives and approaches
WP 3: implementation of privacy policies

Challenges :

- Computing power limitations : need for specific cryptographic algorithms (authentication, confidentiality, integrity)

- Memory limitations : need to minimize the amount of logged data (without compromising log analysis and legal acceptance …)

- Ad-hoc and spontaneous networks : intermittent connectivity, no central server : need for specific authentication protocols

- No tamper proof hardware : need to rely on pure software means to ensure data protection and log integrity

- Privacy API to allow for the integration of applications with different privacy needs