

Pseudonymous Context-Aware Transport Applications

David Evans Alastair Beresford

Computer Laboratory
University of Cambridge

Outline

1. Introduction: Why Privacy?
2. Example Applications
3. Middleware Services
4. Our Plan

1. Introduction: Why Privacy?

The Problem

- Context-aware applications build models of the world
- These models contain information about people
- People worry about...
 - Where this information is stored
 - Who gets to see it
 - How it is used

Approach I: Access Control

- Only allow appropriate access to the information

but...

Explicit configuration is required \Rightarrow Process is not invisible

Correct configuration is challenging \Rightarrow Errors lead to compromised privacy

Demands trusted infrastructure \Rightarrow Difficult in a multi-domain application

Approach I: Access Control

- Only allow appropriate access to the information

but...

Explicit configuration is required \Rightarrow Process is not invisible

Correct configuration is challenging \Rightarrow Errors lead to compromised privacy

Demands trusted infrastructure \Rightarrow Difficult in a multi-domain application

Approach I: Access Control

- Only allow appropriate access to the information

but...

Explicit configuration is required \Rightarrow Process is not invisible

Correct configuration is challenging \Rightarrow Errors lead to compromised privacy

Demands trusted infrastructure \Rightarrow Difficult in a multi-domain application

Approach I: Access Control

- Only allow appropriate access to the information

but...

Explicit configuration is required \Rightarrow Process is not invisible

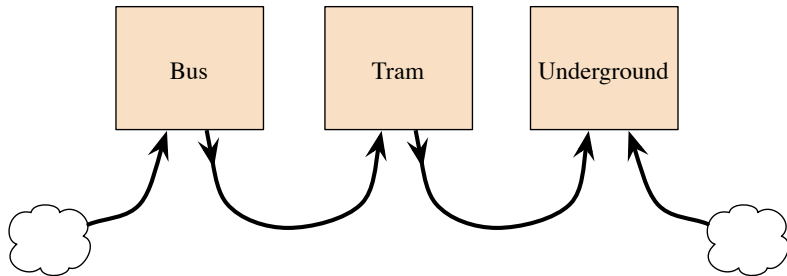
Correct configuration is challenging \Rightarrow Errors lead to compromised privacy

Demands trusted infrastructure \Rightarrow Difficult in a multi-domain application

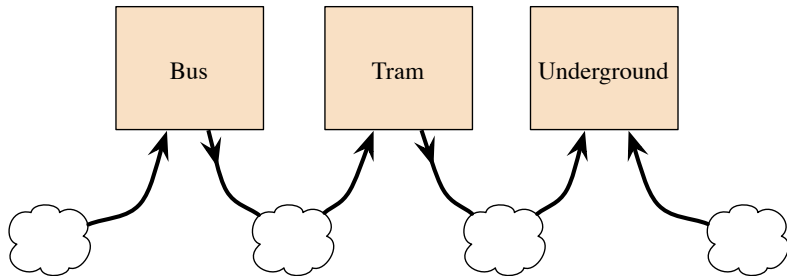
Approach II: Limit Collection of PII

- Ensure that PII doesn't enter applications' context in the first place

Anonymising Personal Information



Anonymising Personal Information



Our Goal

- Build middleware supporting context-aware applications that respect their users' privacy
- Focus is on on transport applications and location information

2. Example Applications

Friend Finder

You want to travel with a friend. Should you get on the next bus?

Meeting Place Recommender

A group of people want to find the “best” meeting place.

Taxi Locator

Use transport infrastructure to enhance taxi service

- Taxi dispatch and routing
- Assist customers (select company, find assigned taxis)
- Predict journey cost

3. Middleware Services

Pseudonym Construction and Distribution

- Associate a pseudonym with...
 - A person or a vehicle
 - A location
 - A group of people, vehicles, or locations
- Pseudonyms are shared, ideally, through socially natural interactions
- Statistical disclosure control to ensure pseudonyms actually provide privacy

Pseudonym Storage

- Store pseudonyms on vehicles
- Pseudonym collation and transfer
- Query list of stored pseudonyms

Pseudonymous GIS

- Perform geographical information system operations on pseudonymous locations, routes, and individuals

4. Our Plan

Our Plan

1. Build the middleware services
2. Use them to implement our example applications
3. Use further applications to exercise the middleware