Virtual Walls: Protecting Digital Privacy in Pervasive Environments

Onur Cobanoglu

09.28.2009
Problem Outline/Motivation

• In pervasive environments, location privacy is only one kind of privacy.

• Through various kinds of sensors, people in pervasive environments leave many kinds of digital footprints.

• Some digital footprints include identifiable information about the user (personal), while some other include generic information (general).
Problem Outline/Motivation

• **Problem:** We want the users of a pervasive environment determine their own privacy policy, in the existence of numerous digital footprints.

• An inexperienced user will need an abstraction of policy which they understand and from which they correctly infer what privacy level to expect.
Solution: Virtual Walls

• The policy abstraction is a metaphor: People intuitively know what privacy level to expect from physical walls, so provide people policies that will provide the privacy levels of physical walls.

• The natural implication is virtual walls around a physical space.
Solution: Virtual Walls

- A virtual wall will provide only as much privacy as a physical equivalent may provide and this defines the capabilities of the system.

- **Example 1:** Bob sitting in his office with translucent walls around (the example from the paper). A privacy breach?
Solution: Virtual Walls

• Example 2:
  – Alice has opaque virtual walls around her dorm room.
  – Alice turned the volume of the music too loud.
  – Bob – her neighbor downstairs – hits the ceiling with a broomstick saying that “Alice, shut the music down!” Bob has transparent walls around his dorm room.

A privacy breach?
System Architecture

• Digital footprints are extracted by a sensing infrastructure and sent to a context server via secure channels.

• Context server disseminates the digital footprints to querying users, if allowed or not denied by virtual walls defined by users.
Premises for Security

• Context server is trusted for confidentiality and integrity of digital footprints, digital footprints are destroyed when overridden by new ones.

• The system can securely identify the borders of a physical place.

• There are no bugs (i.e. hidden sensors).
Some Definitions

• **Places**: Physical spaces.

  – Atomic or aggregate.

  – Atomic places do not overlap. **Why?**

  – Places have meaningful labels.
Some Definitions

- **Footprints:** Maybe *general* or *personal*.
  - **General Footprints:** Consists of:
    - Description of the footprint
    - Set of places where the footprint originates.
    - Timestamp
    - Value of the footprint.
  - **Personal Footprints:** Includes an additional attribute, the set of *owners*.
    - Description and place of originating form the ID of a general footprint (personal footprint ID includes owners in addition).
    - Footprints can be queried on any combination of attributes.
Some Definitions

• **Virtual Wall**: is defined by:
  – Its owner (a user in the system).
  – The place it encloses.
  – Transparency (*transparent*, *translucent* or *opaque*).
  – An *apply set* (the set of users to which this wall applies).
Some Definitions

• The creator of the wall is owner of the wall.
• Only the owner of the wall can modify the properties of the wall.
• A wall protects personal footprints of only the owner of the wall.
• A wall protects only the footprints originating from the set of places around which the wall exists.
Some Definitions

• An **opaque** wall denies access to general and the owner’s personal footprints to the apply set (can be revoked by new users in the place).

• A **translucent** wall denies access to the owner’s personal footprints to the apply set (default behavior of the system).

• A **transparent** wall **grants** access to the owner’s personal footprints, if they are not blocked by any other wall. **How can this ever happen?**
Complications/Shared Footprints

• What if a personal footprint belongs to multiple users (which is possible by the footprint model)?

• **Solution:** Each member of the set of owners has a virtual wall in the place and the most restrictive wall applies for the shared personal footprint.
  – If transparencies of walls are conflicting, each owner is notified.
Complications/Conflicting Walls

• Multiple walls belonging to the same owner for the same footprint and apply set, with different transparencies:
  – For footprints originating from a single place: Solved at creation time.
  – For footprints with multiple origins: The most restrictive wall apply.
Complications/Conflicting Walls

• Opaque wall of one user conflicts with translucent or transparent walls of other users: General footprints cannot be accessed by the apply set.
  – Is this really a conflict?
  – Can you see any problem here?
A Scenario

• Alice is in meeting with Bob in a room around which Alice has an opaque wall and Bob has a transparent wall.

• There are audio sensors and sensing infrastructure can distinguish the voices of different users, considering personal speech as a personal (not shared) footprint.

• Bob says: “OK Alice, what did Mr. X say to you?”
  – A possible counter-argument: This is a matter of incorrect classification of footprints.
What about this?

- Alice, Bob, Cindy and Dave meet in a room, around which Alice, Bob and Cindy have transparent walls and Dave has a translucent wall. Say Alice, Bob and Cindy leave personal footprints not shared by Dave.

- An adversarial with background knowledge can infer that the fourth person is Dave.
  - A possible counter-argument: OK, that’s easier. Dave should create an opaque wall
Gist of the Problem

• These possible solutions are hacks to the problem.

• The system does not comply with the declared metaphoric abstraction (i.e. what you expect from a physical wall is not always what you get from a virtual wall).
Evaluation

Since the primary motivation was comprehensibility and usability of the privacy policies, experiments tested the ease of understanding and use of virtual walls, along with tests of usability of a GUI.

- **Ease of understanding virtual walls**: Participants guessed the kinds of information that a user can have through already created virtual walls.
- **Ease of use of the virtual walls**: Participants asked to create virtual walls for predefined privacy requirements.
- **Ease of use of the GUI**: Participants asked to create predefined virtual walls via a AJAX based GUI running on a web browser.
Evaluation - Results

Table 1. Overall study responses

<table>
<thead>
<tr>
<th>Section</th>
<th>Correct responses</th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Ease of understanding the model</td>
<td>99.4%</td>
<td>90.1%</td>
<td></td>
</tr>
<tr>
<td>2. Ease of use of the model</td>
<td>96.3%</td>
<td>90.5%</td>
<td></td>
</tr>
<tr>
<td>3. Ease of use of the user interface</td>
<td>97.2%</td>
<td>95.5%</td>
<td></td>
</tr>
</tbody>
</table>

Table 2. Successful responses by topic of question

(a) Section 1, understanding the model

<table>
<thead>
<tr>
<th>Topic</th>
<th>Personal Footprints</th>
<th>General Footprints</th>
</tr>
</thead>
<tbody>
<tr>
<td>Transparent</td>
<td>95.7%</td>
<td>91.3%</td>
</tr>
<tr>
<td>Translucent</td>
<td>93.5%</td>
<td>88.0%</td>
</tr>
<tr>
<td>Opaque</td>
<td>100.0%</td>
<td>95.7%</td>
</tr>
</tbody>
</table>

(b) Section 2, use of the model

<table>
<thead>
<tr>
<th>Topic</th>
<th>Correct responses</th>
</tr>
</thead>
<tbody>
<tr>
<td>Transparent</td>
<td>93.5%</td>
</tr>
<tr>
<td>Translucent</td>
<td>94.8%</td>
</tr>
<tr>
<td>Opaque</td>
<td>86.96%</td>
</tr>
</tbody>
</table>
# Evaluation - Results

## Table 3. Time to complete interface tasks

<table>
<thead>
<tr>
<th>Section</th>
<th>CS participants</th>
<th>non-CS participants</th>
<th>non-CS removed</th>
</tr>
</thead>
<tbody>
<tr>
<td>3a. Creating a wall</td>
<td>30.4 (13.7)</td>
<td>31.3 (19.2)</td>
<td>27.7 (11.9)</td>
</tr>
<tr>
<td>3b. Modifying a wall</td>
<td>11.6 (5.8)</td>
<td>15.1 (21.3)</td>
<td>10.9 (10.4)</td>
</tr>
<tr>
<td>3c. Deleting a wall</td>
<td>11.1 (4.2)</td>
<td>11.3 (9.6)</td>
<td>9.3 (4.7)</td>
</tr>
<tr>
<td>3d. Resolving a wall conflict</td>
<td>31.4 (11.2)</td>
<td>37.0 (26.2)</td>
<td>34.6 (23.5)</td>
</tr>
</tbody>
</table>

## Table 4. Successful responses for interface tasks

<table>
<thead>
<tr>
<th>Section</th>
<th>Correct responses</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>CS participants</td>
</tr>
<tr>
<td>3a. Creating a wall</td>
<td>94.1%</td>
</tr>
<tr>
<td>3b. Modifying a wall</td>
<td>100.0%</td>
</tr>
<tr>
<td>3c. Deleting a wall</td>
<td>100.0%</td>
</tr>
<tr>
<td>3d. Resolving a wall conflict</td>
<td>100.0%</td>
</tr>
</tbody>
</table>
Strengths/Weaknesses

• **Strengths:**
  – Highly comprehensible and easy to use policy abstraction.
  – Flexible, allows multiple walls co-exist and walls are defined for specific footprints and specific user set to apply.

• **Weaknesses:**
  – Too many things left for future consideration.
  – What you expect from physical walls is not always what you get from their virtual counterparts.