Controllable Privacy and Security for Pervasive Computing

**MOTIVATION**

- Users interact with a large and growing number of policies, e.g. mobile location-based applications, social networking privacy policies, home firewalls and routers
- But end users have great difficulty specifying and maintaining their security and privacy policies
- Poor specification can lead to security breaches or unintended disclosure of private information

**OBJECTIVES**

- Develop interface technologies that help users maintain their security & privacy policies
- Evaluate tradeoffs between expressiveness, tolerance for errors, burden on users and overall user acceptance.
- Validation through frequent and extensive user studies – lab studies as well as studies “in the wild”

### Visualization

<table>
<thead>
<tr>
<th>Expandable grids allow users to effectively view and manipulate policies at different levels of granularity, enhancing the ability to identify policy errors &amp; supporting conflict resolution.</th>
<th>New family of machine learning (ML) techniques provide users with suggestions of how to improve their policies.</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Benefits:</strong> Improved accuracy &amp; heightened sense of user control.</td>
<td><strong>Benefits:</strong> <em>Moves away from traditional “black box” configuration of ML algorithms</em></td>
</tr>
<tr>
<td>•Higher accuracy measured across 14 Windows file permission configuration tasks – up to 80% improvements</td>
<td>•Users retain control over policy changes (e.g. avoiding poor generalizations) &amp; work hand-in-hand with system on common model</td>
</tr>
</tbody>
</table>

### Current Application Domains

- **Contextual Instant Messenger**
  Users inquire about each other’s context (interruptability, location, and current task) through an instant messaging service.

- **PeopleFinder**
  Laptop and cell-phone users can selectively share their locations with others, subject to privacy policies they can refine over time.

- **Phone-Based Access Control**
  Smart phones act as tokens by which users grant access to rooms, subject to security policies maintained directly on the phones

**RESULTS AND BROADER IMPACT**

- Broad adoption of many mobile and pervasive computing applications hinge on users feeling that they have adequate control over their privacy and security
- Our policy authoring solutions have been shown to empower users to more accurately define their policies in different domains