CS 1699: Privacy in the Electronic Society

Homework 2

Released: Monday, April 2

Version 1 due: Thursday, April 5, before class

Version 2 due: Tuesday, April 10, 11:59 PM

Note: This assignment is submitted electronically, unlike other homework assignments.

Description

In this assignment, you will consider an application that uses location sharing to provide a service to its users. You will design the privacy features and controls that enable your application to provide utility to its users while protecting their privacy as much as is feasible.

You should assume that your users have a relatively high level of technical proficiency and privacy awareness. That is, you are designing a system for a niche that could be approximated as, “CS 1699 PES students.” Assume that your users have some programming experience, are aware of the dangers of privacy violations, and desire a functional yet secure solution. This means you may use more complex techniques to the following tasks than the average user would appreciate, including privacy protections that are only convincing to users within this niche.

To present the design of your system, consider each of the following topics.

1. First, describe your application in depth, emphasizing its use of location data. What data is collected, and how is it used? What utility do your users derive from this sharing? Is it a social system, or is the location data shared only with the service? Why would users want to sign up for your service?

2. Describe the location privacy configuration options available to your users. Can they balance utility derived vs. privacy preserved to match their own preferences? Do users set a simple privacy parameter, or do they write a full policy regarding who can access their data and when? Describe the interface(s) used to make these configuration changes. Finally, consider the effect on the utility of the service as these options are changed. If you will not provide any configuration options, describe some options you considered, and why you chose not to include them.

3. Describe any technical obfuscation or anonymization techniques your service will use to protect its users’
privacy (e.g., mix zones, adding noise). Explain how your approach protects your users, and any effect it has on the utility of the data collection. How do you continue providing the same (or similar) service with obscured data? How will you convince your users that their privacy is actually protected, and that your service is not claiming to obfuscate while reconstructing the data in question? If you do not include any obfuscation techniques, describe some options you considered, and why you chose not to include them.

4. Consider any interactions between your service’s user preferences and obfuscation techniques. Will preferences de-anonymize users or re-link separate pseudonyms? Will obfuscation work better for users with certain configurations? Can users configure the degree to which they are obfuscated or anonymized? Why do these specific designs combine to create a secure system that technical, privacy-aware users would feel comfortable using while also deriving worthwhile utility?

5. Conclude your paper with a paragraph summarizing your system and advertising it to your target user base. Given all of the above considerations, why should someone choose to use your system?

### Grading

<table>
<thead>
<tr>
<th>For each event</th>
<th>Points</th>
</tr>
</thead>
<tbody>
<tr>
<td>Description</td>
<td>10</td>
</tr>
<tr>
<td>Configuration</td>
<td>25</td>
</tr>
<tr>
<td>Obfuscation</td>
<td>25</td>
</tr>
<tr>
<td>Combination</td>
<td>25</td>
</tr>
<tr>
<td>Conclusion</td>
<td>15</td>
</tr>
<tr>
<td><strong>Total</strong></td>
<td><strong>100</strong></td>
</tr>
</tbody>
</table>

Your grade will be split between Version 1 (submitted by April 5, before class) and Version 2 (submitted by April 10, 11:59).

### Submission

Upload your report as a PDF file to the Box folder created for you with the name `cs1699-hw2-abc123`, where `abc123` is your Pitt username. Version 1 will be graded based on whatever is uploaded before I leave my office for class on Thursday, April 5, but your Box folder will remain writable. On Tuesday, April 10, at 11:59, your Box folder will be made read-only, and Version 2 will be graded based on the final submission.