RuzenaFit: Exercising the Limitations of Privacy

Maurice Grant, Girum Ibssa, Ferda Ofli, Posu Yan, Aaron Bestick, Ruzena Bajcsy

Ithaca College | Cal Poly, San Luis Obispo | University of California, Berkeley

Introduction

We present an gamified, privatized Android exercise app as our implementation of two research questions:

Questions

• "Can we incentivize users to privatize or de-privatize their sensitive information?"
- To promote sharing *more* information, provide more "points" for more information.
- To promote sharing *less* information, simply submit their information to the public (live web app & Facebook wall).

• "How effective can competition be as an incentive to get at-risk patients to exercise?"
- All user data uploaded to a central server
- Real time rankings of users available both from the client and the web app.

Challenges

• A light privacy framework needed to be built to persist only as much sensitive data as the user wished.
• Players only upload data when there is an Internet connection available – player "rankings" can be appear to be out of date to other players in the competition.
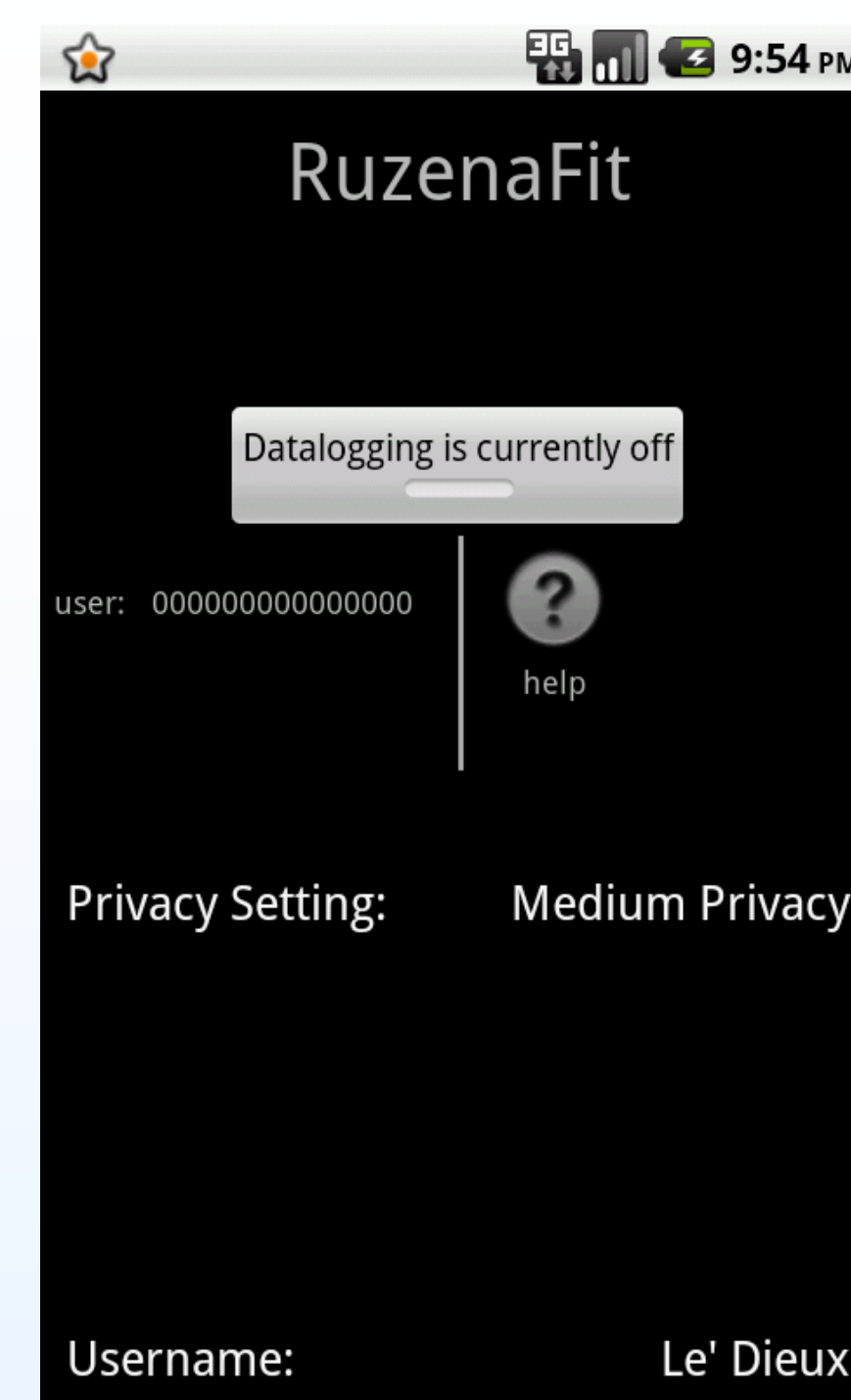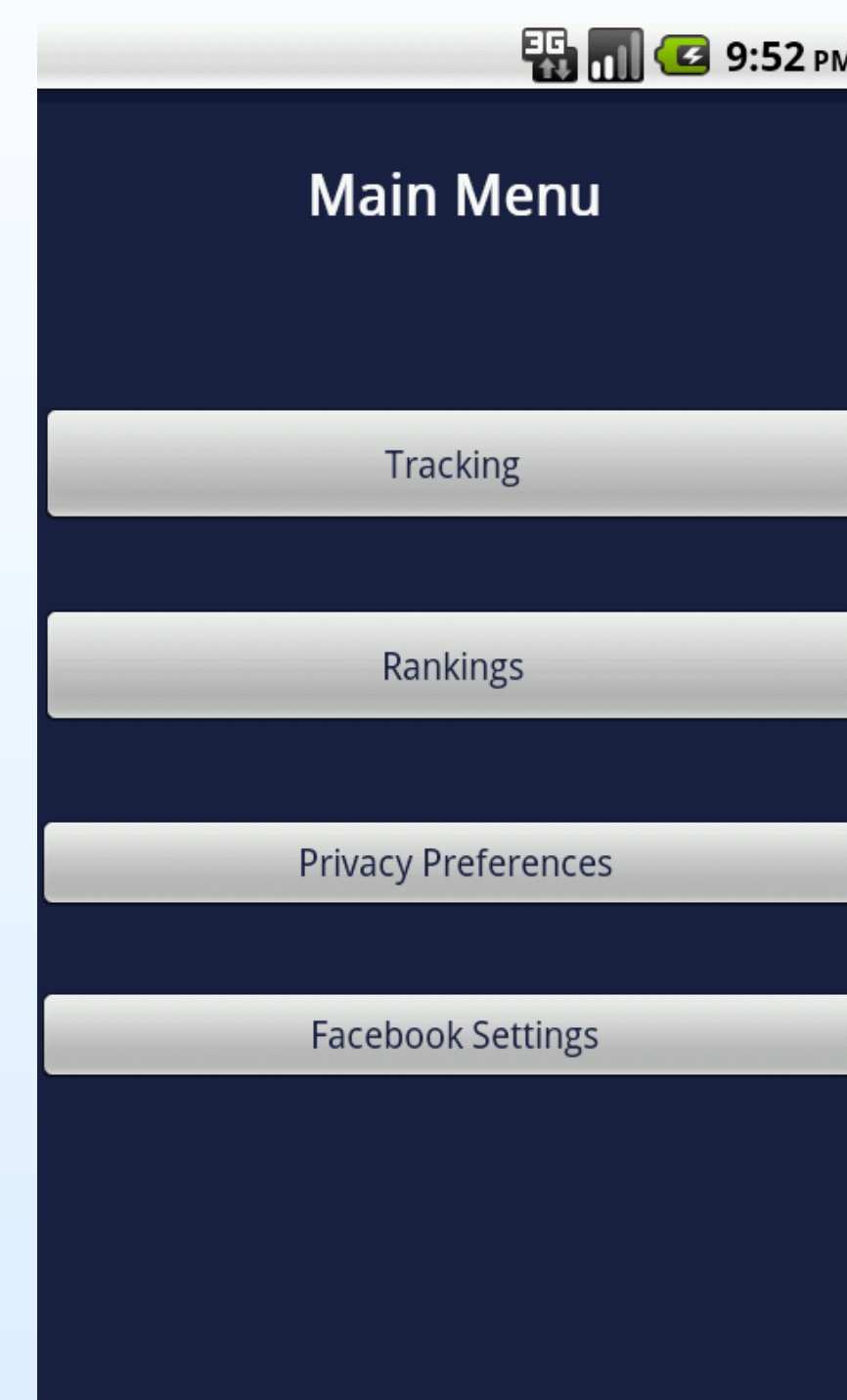
Design

Goals

• Establish a framework for privatized sensor data collection
• Modularize sensor collection in the app, in the hope that the code base can be used in future applications in the medical domain.
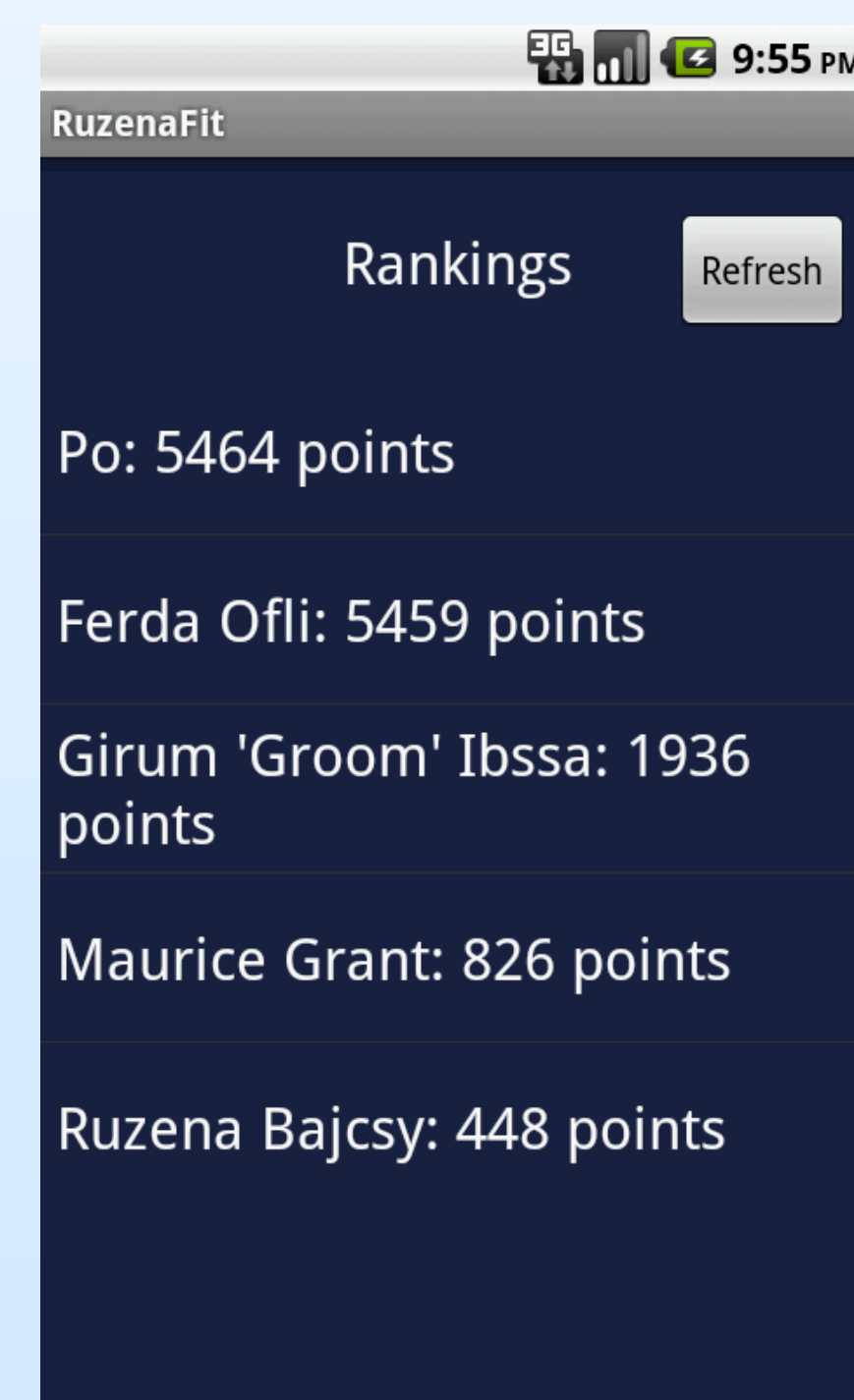
System Components

• Android client
- Each player has distributed to him an Android device
- The device provides sensor and network interfaces to track and upload data
• Web server (back end and front end)
- Back end exposes user data via a simple REST API, specific to this application and its privacy framework
- Front end uses remote procedure calls to access same datastore, displaying real-time analysis of data
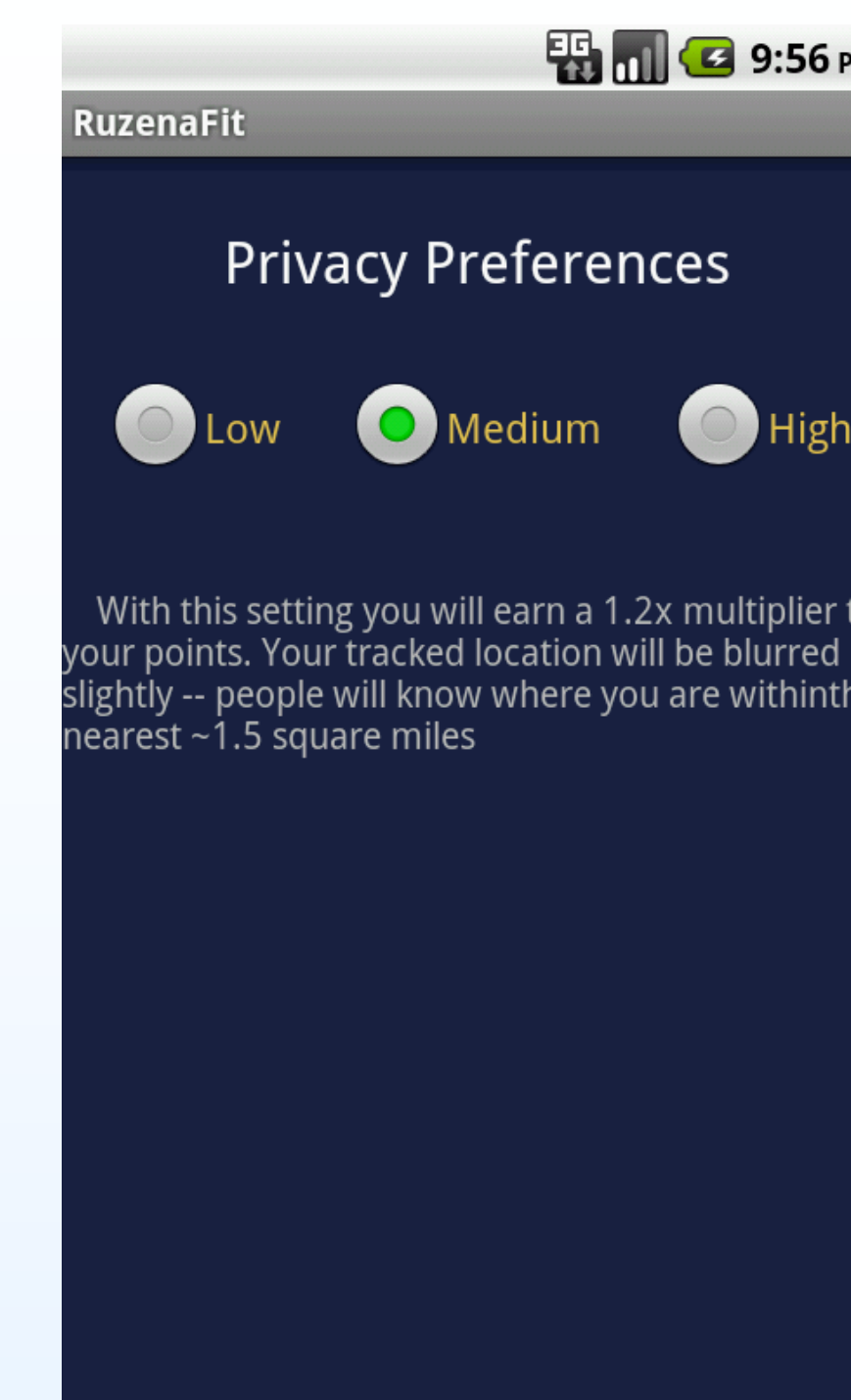
Storyboard Overview

Main Menu
- Tracking
- Rankings
- Privacy Preferences
- Facebook Settings

RuzenaFit
Datalogging is currently off
user: 000000000000000
help
Privacy Setting: Medium Privacy
Username: Le' Dieux

Tracking screen – Designed to be as autonomous as possible, the user starts the datalog once. From then, she can put away the phone until she wants to change her privacy settings.

Privacy Preferences
Low Medium High

With this setting you will earn a 1.2x multiplier to your points. Your tracked location will be blurred slightly -- people will know where you are within the nearest ~1.5 square miles
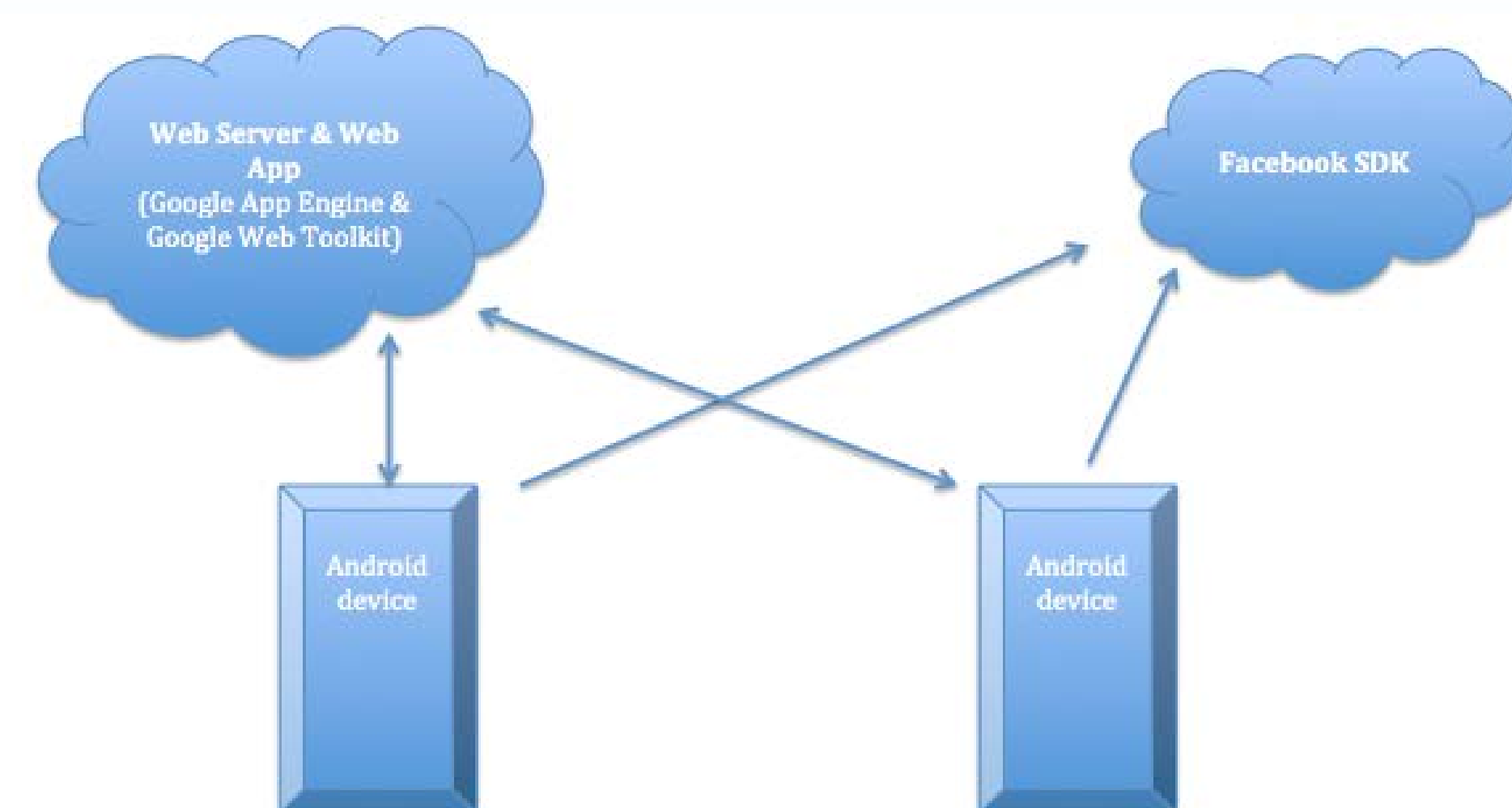
Privacy screen – The crux of our business logic, here is where the player sets his privacy preference at any point in the tracking. He may not begin tracking until this parameter has been set.

RuzenaFit
Rankings Refresh
Po: 5464 points
Ferda Ofli: 5459 points
Girum 'Groom' Ibssa: 1936 points
Maurice Grant: 826 points
Ruzena Bajcsy: 448 points

Ranking screen – This page automatically refreshes with the most up-to-date rankings that the server has on-hand.

RuzenaFit
Facebook Settings
Login with Facebook
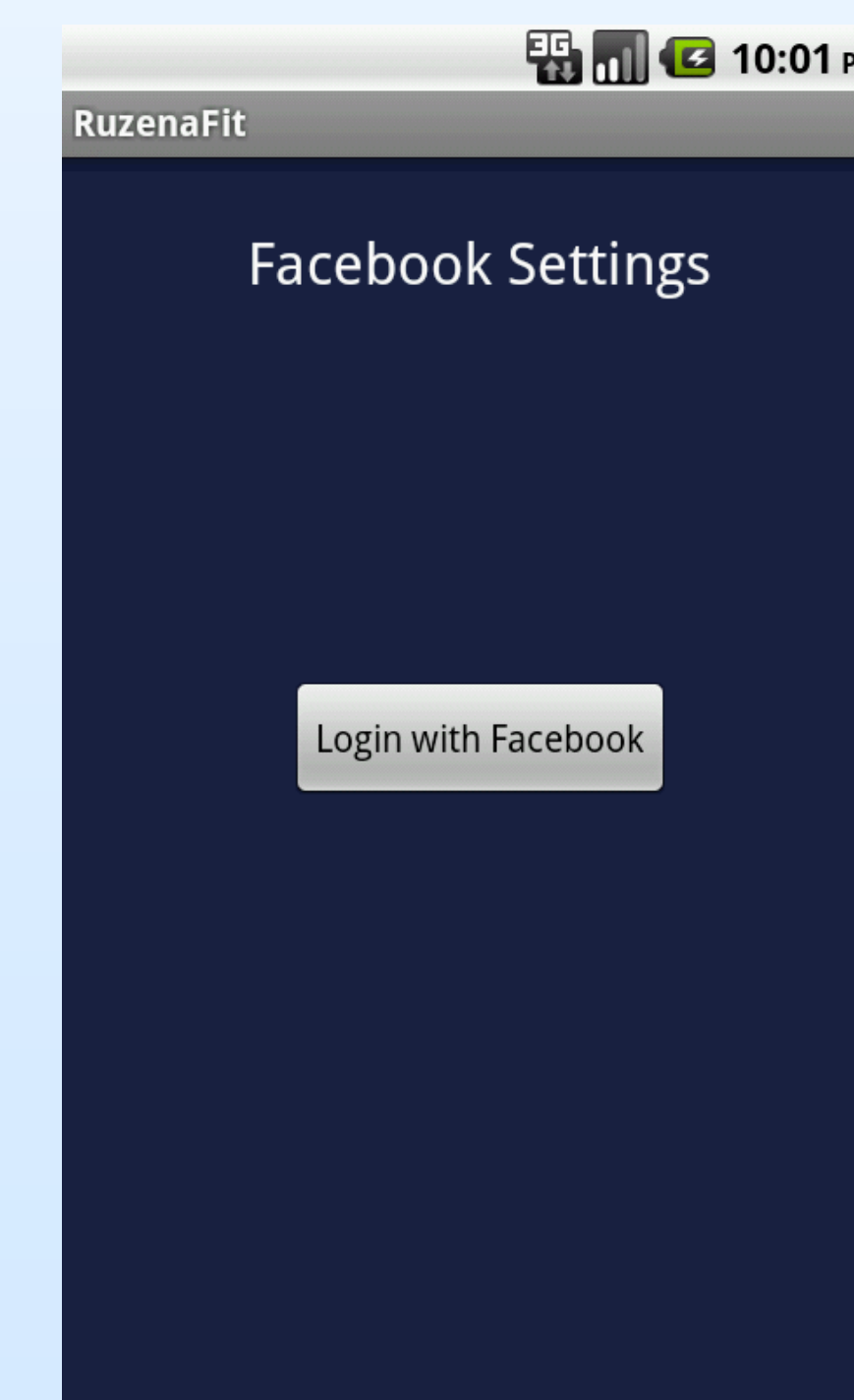
Facebook settings – Players must login to their Facebook account to play this game, as part of our social engineering to de-incentivize sharing information. This was done without sacrificing modularity.

Software Hierarchy Overview

Web Server & Web App (Google App Engine & Google Web Toolkit)
Facebook SDK
Android device
Android device

Phones do not "talk" to each other. Rather, all user data goes through the server, with as much detail as each Android device specifies with its privacy setting at that point.

Sample Chart Data

Maurice
Girum
Firda
Ruzena
Po

e.g. "Scores" per player per day