Semester Thesis — Mobile currency for dealini.ch

About dealini.ch

dealini.ch is redefining the online deals space. Part online game, part shopping site, on Dealini you trade coupon cards to get as much as 100% off the deal you want. An active community with over 50.000 registered users is collecting, trading and haggling over the best offers. A virtual currency, the “Dollarini”, is used for real-world payments, in-game trading and as a reward for player activities.

dealini.ch mobile app

To allow our users to benefit from using dealini.ch on the go, a native mobile app is being developed in-house. We primarily focus on iOS, as most of our Swiss users have an iPhone. Core features are displaying of collectable deals and trading coupon cards with other players.

The Project

To enable a much broader use of Dollarini, they should be brought to the physical world. This thesis covers the development of a mobile app which enables our users to locate and collect Dollarini in the real world, assuming a working data connection when collecting them (“online”). Together with this mobile app, a simple backend for our external partners should allow them to drop Dollarini at various locations (creating a “Dollarini well”), e.g., their brick-and-mortar shop.

The app must be secured against man-in-the-middle attacks, and it must be able to detect simple location spoofing attacks. Furthermore, a good user experience is key, as it needs to account for the inherent fuzziness of mobile localization (especially in urban areas). A good balance between the requirements of our customers (e.g., having players visiting the shopping window of shop owners) with those of our users has to be found. Offline capabilities should be introduced where they are useful.

Environment

Development will take place at the Dealini (Schweiz) AG office in Schlieren.
The mobile app will be developed using Objective-C & XCode, based on the already existing native iOS app. A suitable development environment (hardware & software) as well as graphical designs will be provided as needed.
The backend (management interface and RESTful API) is developed with Pyramid, a web framework based on Python.

Contact

Dr. Martin Geisler <martin.geisler@dealini.ch>

Threat Model

The app runs on an untrusted platform (i.e., on a jailbroken device), but the binary is assumed to be safe (external app data is not). Therefore we expect that an attacker could eavesdrop on the communication between the app and our API servers, either by passively monitoring traffic (and possibly using this information in a replay attack), or by actively intercepting communication (Man-in-the-Middle) and impersonating API servers or the app. Since the platform is considered to be untrusted, an attacker could also try to spoof the current location of the device.

As an attacker we expect a casual gamer who is using pre-built tools (i.e., existing apps) to cheat in games, but who has not the know-how to carry out lower-level attacks by himself (i.e. disassemble the binary and inject his own code).

Tasks

(*italics*: nice-to-have features)

- General
  - secure against MitM & location spoofing
- Phase 0: Drop
  - possible from the administrator interface (a.k.a. “dashboard”) on a map view
  - “wells” configurable in many ways (time-/amount-based, per-user or total limits...)
  - placing anywhere in the world
  - handling arbitrary goods (focus on Dollarini, but extensible to virtually anything)
- Phase 1: Discover
  - map view with suitable level of detail
  - offline caching of discovered wells
  - detail view for wells with additional information
  - map interaction possible without account/login
- Phase 2: Collect
  - locate device and enable pickup
  - verify pickup online
  - update app state (e.g., retrieve current Dollarini count from server)
  - login only if needed by well
  - simple collection statistics, both for the user and in the administrator interface
  - server-side offline algorithm to detect location spoofing

Evaluation Criteria

- Basic runtime statistics (CPU/memory/bandwidth/battery usage, speed)
- Robustness against eavesdropping and simple location spoofing attacks