Design

Overview

Purpose and Goals
- Brief Description: An app to organize and split the group purchase of a gift for someone.
- Key Goals and Purpose: Facilitate easy and orderly planning for gifts
- Motivation:
  - Allows for and improves simplicity in group discussion and selection of gift
  - No prominent sites that serve to fix this problem exist. We found one that requires all users to have Facebook accounts.
  - Applicable to the creators' network - college students are poor and tend to split the costs of gifts

Context Diagram

Concepts

Key Concepts
- Organizer: create gift-fundraising event, moderate discussion, final decision on gift, all
roles of members in addition.
• Members: pledge money, discuss and propose gifts, vote.
• Online stores: provide products.
• Products: serve as targets of discussion and as the presents.

Data Model

Textual constraints:
• A user may be both an organizer of 0 or more groups and a member of 0 or more groups.
• A member may only comment & vote on proposals that are in an active group
• An active group turns into an inactive group when the group’s deadline has passed
• The Organizer is the creator of the group. S/he may add/delete members.

Behavior

Feature Descriptions for UGift
• Centralize your ideas: Decide a gift for a mutual friend with UGift’s online voting system and discussion forum.
• Keep it a secret: As the gift manager, you can choose the friends involved in the process,
set deadlines for them, and record payments made to you.

- **Stay in your budget**: You can state your maximum budget and change this number any time before the deadline.
- **Split Costs Efficiently**: If you raise more than enough money, the cost-splitting system maximizes fairness while still ensuring that you will never pay more than your named price.

### Security Concerns

**Security Concerns:**

- Gift and group isolation - users should not be allowed to see a particular gift or group discussion page if they are not authorized
  Prevented by checking if user is logged in and if the user has permission to access the appropriate URL’s, via any HTTP request.
- User Protection - Others cannot easily obtain user information.
  Prevented by password salting & hashing.

### Threat Model:

- Cookies are encrypted; an attacker cannot guess the cookie for a session, so they cannot forge someone's credentials and view gifts/product ideas they are not authorized to.
- An attacker does not have unlimited time and so cannot guess both the salt and the hash for user's credentials.

### User Interface

**Wireframes for application**

- Log in screen

  ![Login Screen](image)

- Create account screen
Purpose and Goals

UGift is an online app to help a group of people select a gift, for a person (or perhaps for an organization or for another group). It supports assembling the group, making and sharing suggestions for the gift, agreeing on the gift, and dividing the costs. It does not provide the actual purchase of gifts or transfer of payments.

The purpose is to simplify the process of selecting a gift, especially amongst a large number of people, who may not even know each other. Goals include: centralizing the state of the deliberation process (and the list of gift suggestions) in a single, attractive web site; making it easier and more pleasant to negotiate the size of the financial contributions; and (perhaps) also tracking whether members of the group have made their contributions to the payment.

Context Diagram

Key Concepts

**Cabal:** An ad hoc group of users that join together to select a gift. A cabal is associated with only one gift, so there is no separate concept of a gift, ruling out the possibility of a cabal deliberating over several distinct gifts. A cabal has a name chosen by its creator used to distinguish it in the UI from other cabals created by the same person.

**Item:** Something that can be given as a gift. It may be a concrete item (e.g., a book), a service (e.g., an airline flight, a massage) or perhaps a coupon. The item need not be a commodity; it
may be a one-off (eg, a piece of art, or a craft object on Etsy.com). An item must be identifiable by a URL to an online retailer. Generally, this will preclude an item consisting of multiple things, unless (a) they are already packaged together for sale as a single item by the retailer, or (b) the retailer’s website provides a facility to save a shopping cart and provide a link for sharing it.

**Descriptor:** A URL that points to an item. Ideally, the result of issuing a query to such a URL will be a single web page that shows an image of the item. The descriptor need not be a permanent link, but should persist (TBD) at least for the length of time for which typical deliberations last (a month?).

**Pledge:** Users provide a “pledge” to indicate the upper and lower bounds of their contributions. Pledges are not item-specific; rather a single pledge is made by each user for all the items under consideration. Pledges can be private or revealed to other members of the cabal (TBD) and are used to constrain the final choice of item (TBD), and perhaps also the display of suggestions (TBD).

**Policy:** The app might provide different options for how pledges are treated (private or public) and how costs are divided. For example, each member of the cabal might pay the same amount, with the cost of the selected item being at most the number of members multiplied by the smallest pledge; or members might pay different amounts according to some scheme.

**Object Model**

Additional constraints:
— At most one vote per member/item pair
**Feature Descriptions**

**Managing cabal.** Users become members by signing up for the app, and can then form cabals by inviting others, either who are already members, or to become members. Members can belong to multiple cabals, and can (TBD) drop out of a cabal. Each cabal has a single creator who issues all invitations to join and is responsible for closing (TBD) the cabal when the gift has been chosen.

**Pledging.** A member makes a pledge on joining a cabal, and can (TBD) change his or her pledge. The organizer can set in advance a range on acceptable pledges (TBD).

**Making suggestions.** Any member can add a suggestion of an item to a cabal, by providing a descriptor, a price, a title, and optionally a brief textual description. Suggestions cannot (TBD) be withdrawn.

**Voting and commenting.** Members can indicate using up and down votes which items they prefer. They can also make comments about individual items.

**Choosing gift.** The organizer can choose at any point to select an item from amongst the suggestions; the choice is then communicated by the app (by email, TBD) to the other members. The app does not handle the purchase, nor any protocol for reaching consensus. The organizer is not constrained by the pledges, except insofar as the total cost of the item cannot be more than the sum of the maxima of the pledges (TBD).

**Dividing costs.** The app calculates a cost for each member; for now, this cost is obtained by dividing the total cost amongst the number of members.

**Security Concerns**

The security requirements are that:
— Only invited members of cabal can read or write suggestion, pledging, voting and member profile information. The existence of a cabal may be private or public (TBD).
— Members of a cabal can see only each others’ names, and not email addresses or other profile information. Suggestions and who made them are visible to all members; votes are visible, but not who made them; pledges are not visible except to the organizer (TBD).

Potential risks include:
— Hoax organizers who assemble a cabal to defraud its members.
— Dishonest members who refuse to pay after an item has been selected and paid for.
— Members who manipulate pledges to disrupt item selection (eg, by reducing pledges).
— Conflict of interest: members who direct the cabal to items they’re selling.
— Hackers who break into the system and extract profile information about users for identity theft.
— Hackers who insert themselves into a payment channel between members and organizer, perhaps just using this app for pretexting.
— Spam advertizers gain access and add suggestions of pharma, porn, etc.

Threat model
— Can assume no interest from state actors or criminal syndicates, since only minimal profile information stored (name and email).
— For small cabals, assume that all members know each other well, and communicate out-of-band, so little risk of fraud.
— For large cabals, assume that initiation and completion of the process are by out-of-band communication using existing, trusted mechanisms (eg, class mailing lists), so little risk of fraud succeeding.
— Attempts to spam are very likely.

Mitigations
— Standard strategies to address code vulnerabilities (such as injection, XSRF, etc) and thus reduce risk of spamming.
— Attribute all suggestions in name to member, in order to expose members who leak credentials (eg, to spammers).
— Use access control to prevent even viewing of basic cabal information except to members.
— Make organizer responsible for due diligence on purchase, to ensure no conflict of interest or hoax.
— Prevent alterations of pledges, or allow only with organizer approval (TBD).
— Encourage comments as a means of informal authentication (TBD).

Design Challenges
[For now, just the options; haven’t given pros and cons, or choices made]

**How are large cabals created?** For small cabals, emailing each member with an invitation makes sense. But for a large one (convened eg to make a class gift), not all email addresses might be available.
— Provide public cabals that people can request to join
— Let members invite other members
— Distribute a credential that enables recipient to join, limited in some way (by time period, email domain, ability to answer questions)

**What do pledges mean?**
— The minimum indicates the cheapest gift the member thinks is suitable
— The minimum indicates an amount the member is definitely willing to pay
— The maximum indicates the largest amount the member is definitely willing to pay
— The maximum indicates the largest amount the member may be willing to pay
— Maxima and minima are just preferences, and are not binding

**What if a member drops out or reduces pledge?** This might eliminate items that were
previously acceptable. There is also an issue of breach of contract if the item has already been purchased.
— Forbid changes to pledge (except perhaps with organizer approval)
— Enrich protocol with a “closing phase” in which members approve or disapprove of final selection
— Do nothing special, and rely on social pressure

What if an item is inaccessible? A member might provide a URL that does not reliably bring up item information because: (a) it was never a context-independent URL; (b) the website is unavailable; (c) the item is withdrawn by the seller; etc.
— App tests URL before accepting it
— Organizer can delete suggestions that are inappropriate or failing
— App automatically deletes suggestions if repeated access attempts fail
— Member is required always to upload an image and a textual description

What if member enters incorrect price on uploading suggestion?
— Organizer can modify
— Member can modify own suggestion
— Price is obtained automatically by app from online store, so no price is entered

What if item price changes? This will be especially problematic if pledging is taken to be contractual.
— Organizer can reset the price
— Treat pledges merely as preferences, and handle in comments

User Interface

[Not included]