Project 3: Problem Analysis

Stephen Freiberg

Overview

Purpose and Goals

The system that is being built, Red-Dot, is a comment feature that can be used on sites such as Reddit, New York Times, Quora, and Stackoverflow. This feature allows authenticated users to comment on existing posts, and vote up or down other comments. The comments and posts will be updated without a page refresh so that users can view content as it is added, rather than only when the page is opened or refreshed.

This system will also allow the highest voted, and therefore most popular, comments and posts to "bubble up". This allows a high level of content quality, as the users themselves are voting to determine the best content.

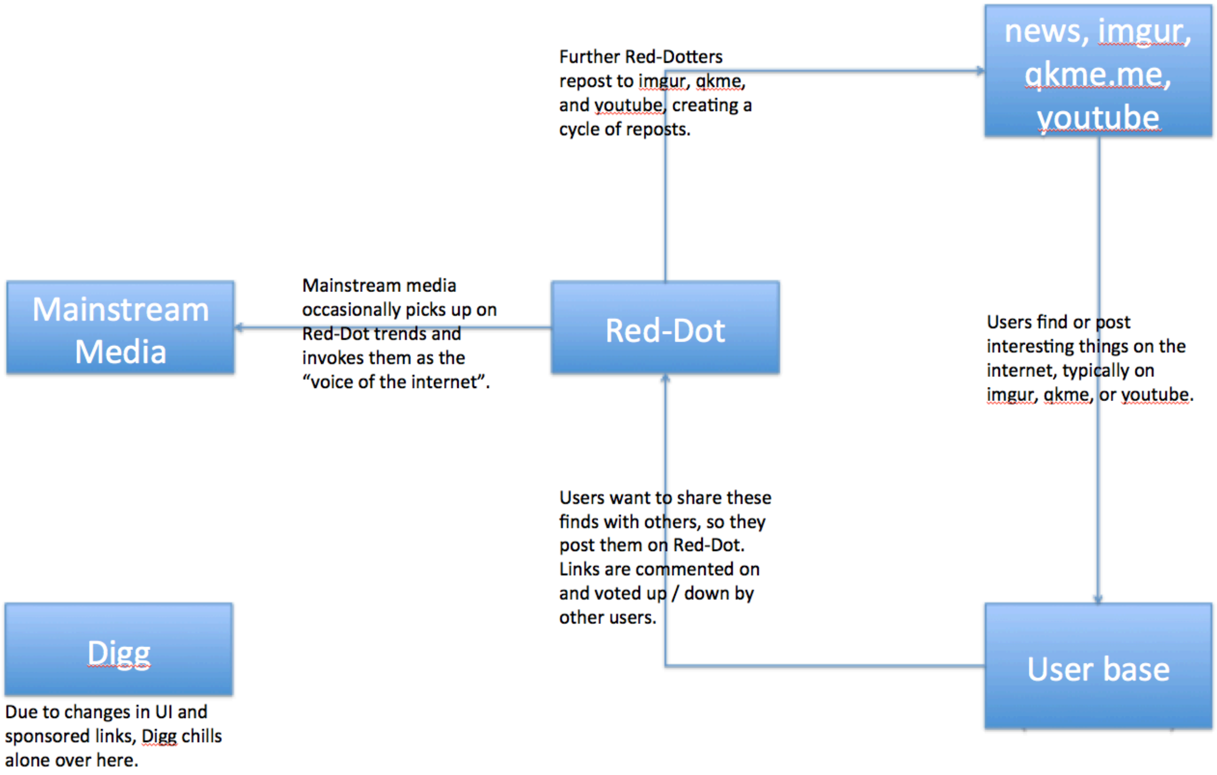
Goals

- Create a simple forum that allows users to submit content and comment on those submissions.
- Allow users to vote on content, and display content such that the most popular comments and posts "bubble up" to the top.
- Users viewing posts and comments should not have to refresh their browsers in order to get the most recent information; this update should occur automatically.
- Red-Dot should have some ability to moderate content, and promote users to submit high quality content.

Motivation for Development

Systems that have existed before Red-Dot have suffered from low quality submissions and spam being added. There can also be a problem of one-time submitters that do not contribute to the community of the forum. Red-Dot plans to tackle these problems by requiring logins to add content, and allowing votes on previously submitted content. Requiring login removes a layer of the anonymity of the internet as well as slows down the one-time contributor or would-be troll. The presence of a login wall thus prevents frivolous users from adding content. Similarly, the presence of voting and ranking of users by popularity helps promote a community of repeat users that are incentivized to submit high quality content that will be useful to the rest of the community.

Context Diagram



Further Red-Dotters repost to imgur, qkme, and youtube, creating a cycle of reposts.

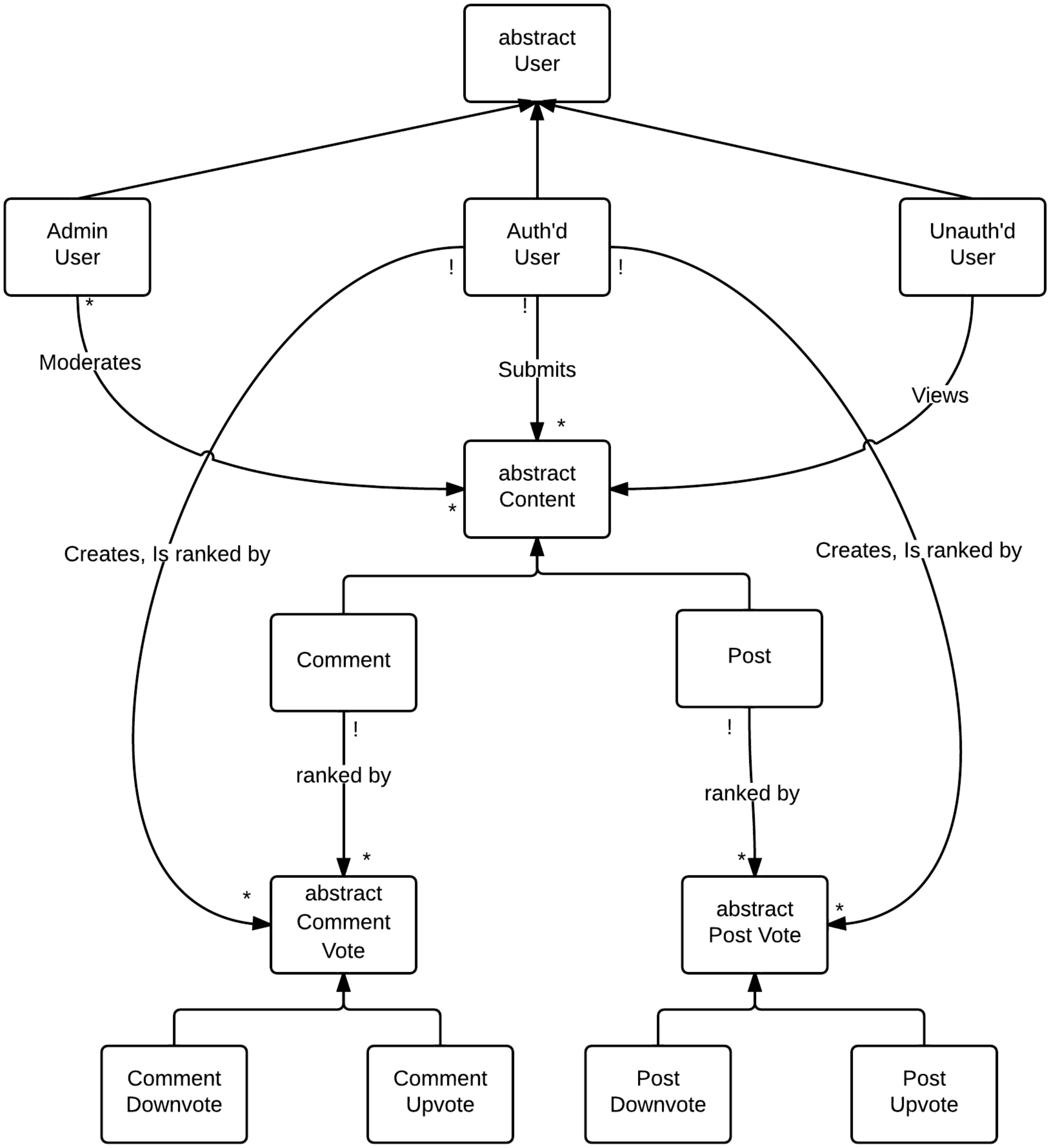
Mainstream media occasionally picks up on Red-Dot trends and invokes them as the "voice of the internet".

Users find or post interesting things on the internet, typically on imgur, qkme, or youtube.

Users want to share these finds with others, so they post them on Red-Dot. Links are commented on and voted up / down by other users.

Due to changes in UI and sponsored links, Digg chills alone over here.

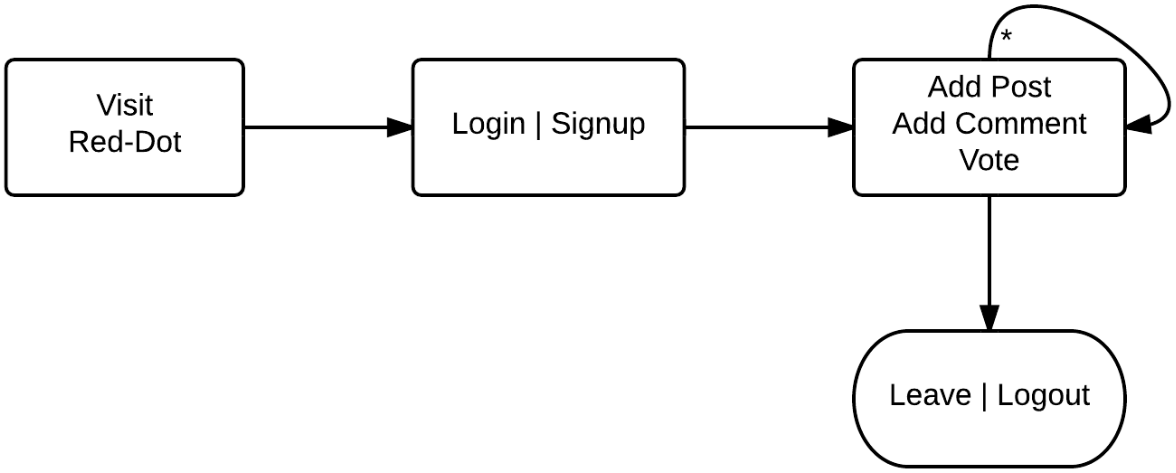
Domain
Object Model

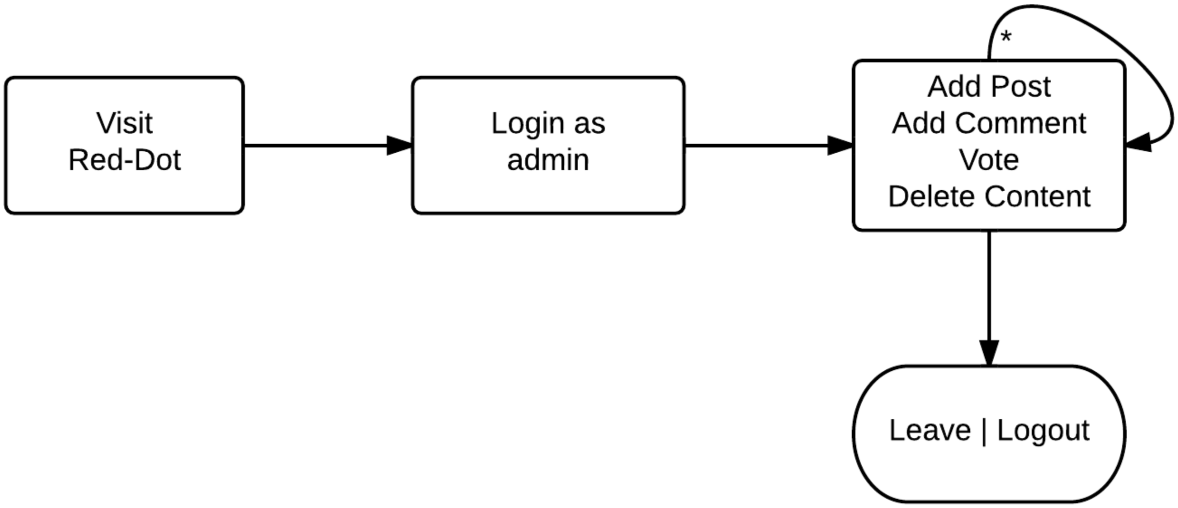


- Users fall into three (not necessarily disjoint) categories. Unauthenticated users can only view content on Red-Dot. Any authenticated users are able to add content and vote on content. Finally, administrator users are able to moderate content. Any user is able to perform the same actions as a user with less privilege (i.e., administrators can still add content).
- PostVotes and CommentVotes capture the popularity of a Content item in the number of users that have recommended it with a vote.

Event Model

Model is indicated as a state machine for Authenticated Users and Administrator Users only. Note that posts and comments are final (cannot be edited, except to be removed by an administrator).





Model is also indicated below as a regular grammar for authenticated users and for admins.
User::= (login | signup) (action)* (logout | leave)
Admin::= (login | signup) (action)* (delete post | delete comment)* (logout | leave)
Action ::= post | comment | vote

Behavior

Feature Descriptions

- Post. This feature allows users to post content in a forum style. This content is titled, and is publicly visible.
- Comment. Users can comment on content in forum style. These comments are shown as in response to a Post.
- Update. The pages containing Post and Comment listings are updated without the user being required to refresh the page. The update occurs on a short polling mechanism.
- Rank. Comments and Posts are shown in order of popularity, which is determined by the number of positive and negative votes attached to that content.
- Top Users. Users are ranked in three categories: link karma, comment karma, and total karma. "Karma" is a measure of the popularity of content that a user has published; upvotes on content positively affect the karma of the original poster.

Security Concerns

Red-Dot, by design, does not store or interact with data that is sensitive to its users (with the exception of a password). Since the history of Posts and Comments is publicly available and there is no monetary value associated with the user accounts, the threat model assumed about attackers is that they are less interested in profiting from, and more interested in breaking, the application.

With the above in mind, the security threats considered are discussed below:

- *Inappropriate content*. A possible threat to Red-Dot would be a prevalence of content that is not suitable for the community. This could include inflammatory speech, advertising, or even inane content that does not add to the site.
  - Inappropriate content will be flagged by administrators and taken down. As the user base grows, it may be necessary to increase the number of administrators or have a model where big contributors to the community can gain administrator privilege. It may even become necessary to include a "Flag this content" button for all authenticated users.
  - Requiring login to use Red-Dot decreases the number of "one-time" contributors that may be less likely to add to the community. In addition, having an account ties all comments and posts back to one person, which introduces a level of accountability and removes a level of anonymity.
  - Including the ability for administrators to ban users would help reduce the number of repeat offenses.
- *Cross Site Request Forgery attacks*. This attack can be prevented by using the keyword "protect_from_forgery" in the ApplicationController.
- *SQL Injection*. Use of the built in ActiveRecord methods will sanitize against SQL injection attacks.
- *XSS Injection*. Use of ERB templates to generate views will allow RoR to automatically escape HTML and only output safe data.

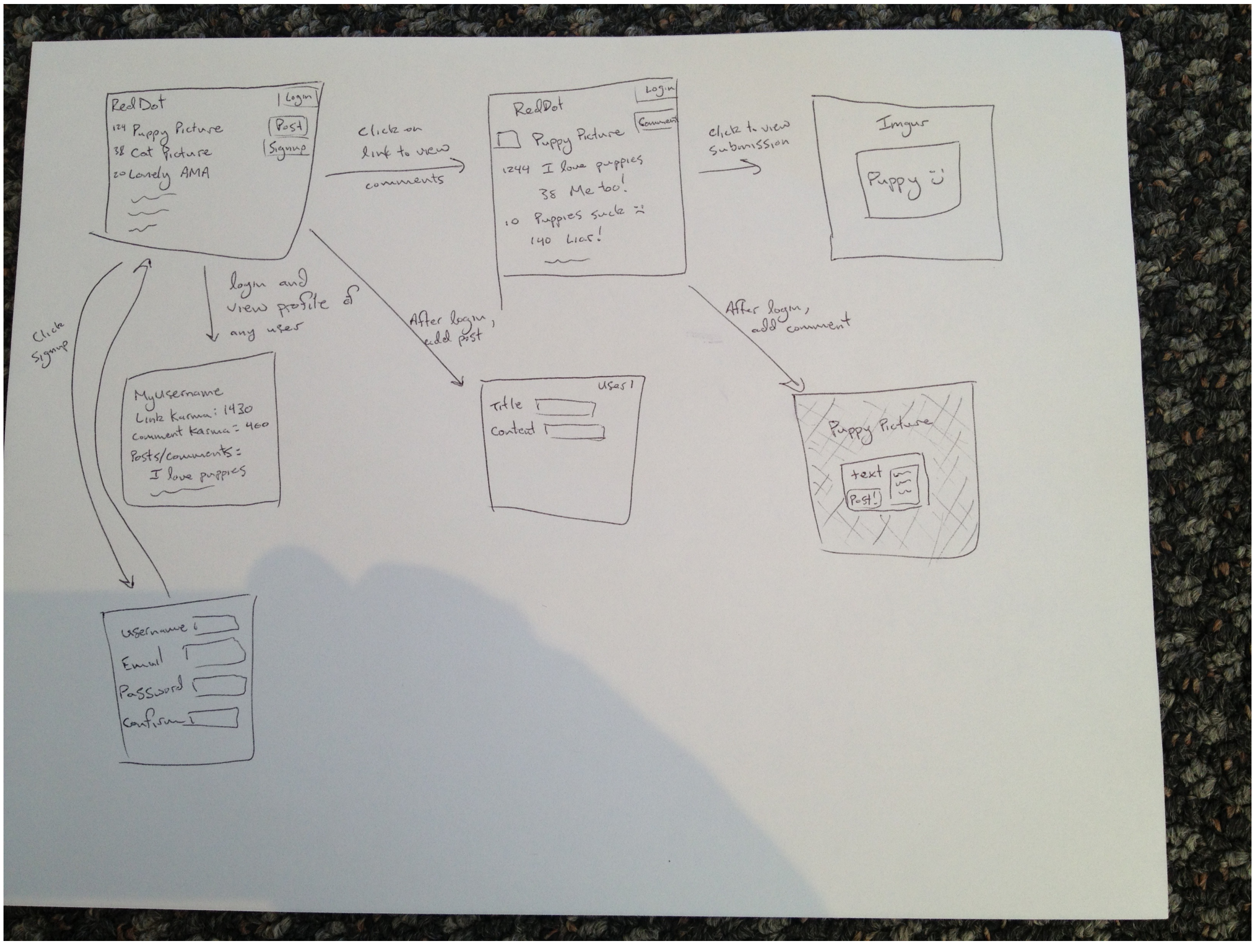
- *Session Replay and Fixation*. Session attacks are prevented by not storing sensitive information in the session, and giving the user a new session every time he or she visits Red-Dot.
- *Mass Assignment*. Mass assignment attacks are prevented with appropriate use of attr_accessible as well as runtime assertions that prevent assignments to blacklisted fields.

Operations

- *Log in*
  - Precondition: User has an account.
  - Frame: User is logged in and given a new session.
  - Post: User is logged in and has posting / commenting ability.
- *Log out*
  - Precondition: User is logged in.
  - Frame: User is logged out, session is destroyed.
  - Post: User is logged out and the browser no longer has posting / commenting privilege.
- *Create account*
  - Precondition: Email address is not already associated with an account.
  - Frame: Account is created to given email address. User is logged in.
  - Post: User is logged in and has posting / commenting ability.
- *Add Post*: Allows authenticated users to add posts to the main website, which each consist of a title and some content.
  - Precondition: User is logged in.
  - Frame: Post is added with given title and content.
  - Post: New post is visible to all users.
- *Add Comment*: Allows authenticated users to add comments to any post.
  - Precondition: User is logged in. Desired Post to comment on exists.
  - Frame: Comment is added with given content.
  - Post: New comment is visible to all users.
- *Upvote / Downvote Post*: Allows authenticated users to vote on posts (approve or disapprove). These aggregate votes are viewable by all users of the site.
  - Precondition: User is logged in. Post exists.
  - Frame: PostVote object is created. Original Poster's karma is affected.
  - Post: Post has new total popularity ranking.
- *Upvote / Downvote Comment*: Allows authenticated users to vote on comments (approve or disapprove). These aggregate votes are viewable by all users of the site.
  - Precondition: User is logged in. Comment exists.
  - Frame: CommentVote object is created. Original Poster's karma is affected.
  - Post: Comment has new total popularity ranking.
- *Delete Post*: Allows administrators to delete questionable or malicious content.
  - Precondition: User is logged in with administrator privilege. Post exists.
  - Frame: Post is destroyed, along with associated Comments and vote objects.

    - Post: Post no longer exists, and neither do any comments or votes associated with it.
- *Delete Comment*: Allows administrators to delete questionable or malicious content.
    - Precondition: User is logged in with administrator privilege. Comment exists.
    - Frame: Comment is destroyed, along with associated vote objects.
    - Post: Comment no longer exists, and neither do any votes associated with it.

User Interface



Addendum: Karma Discussion

Users of this site, Red-Dotters, are able to submit posts and links to the site. Other authenticated users are able to comment on posts and other comments (creating subcomments) as well as upvote and downvote existing comments. Based on the net number of upvotes (upvotes – downvotes), highest rated posts and comments will be presented at the top of the site. Unauthenticated users are able to view comments and posts, but not contribute to the Red-Dot community.

Votes on content submitted by a user contribute to that user's "karma". Each user has two types of karma: link karma and comment karma. The link karma score is affected by the up and down votes on the posts that a user makes. The comment karma score is affected by the up and down votes on the comments that a user makes. These can eventually be used to reward members of the community with “comment influence” that factors in to a more complicated rating formula for posts and comments.