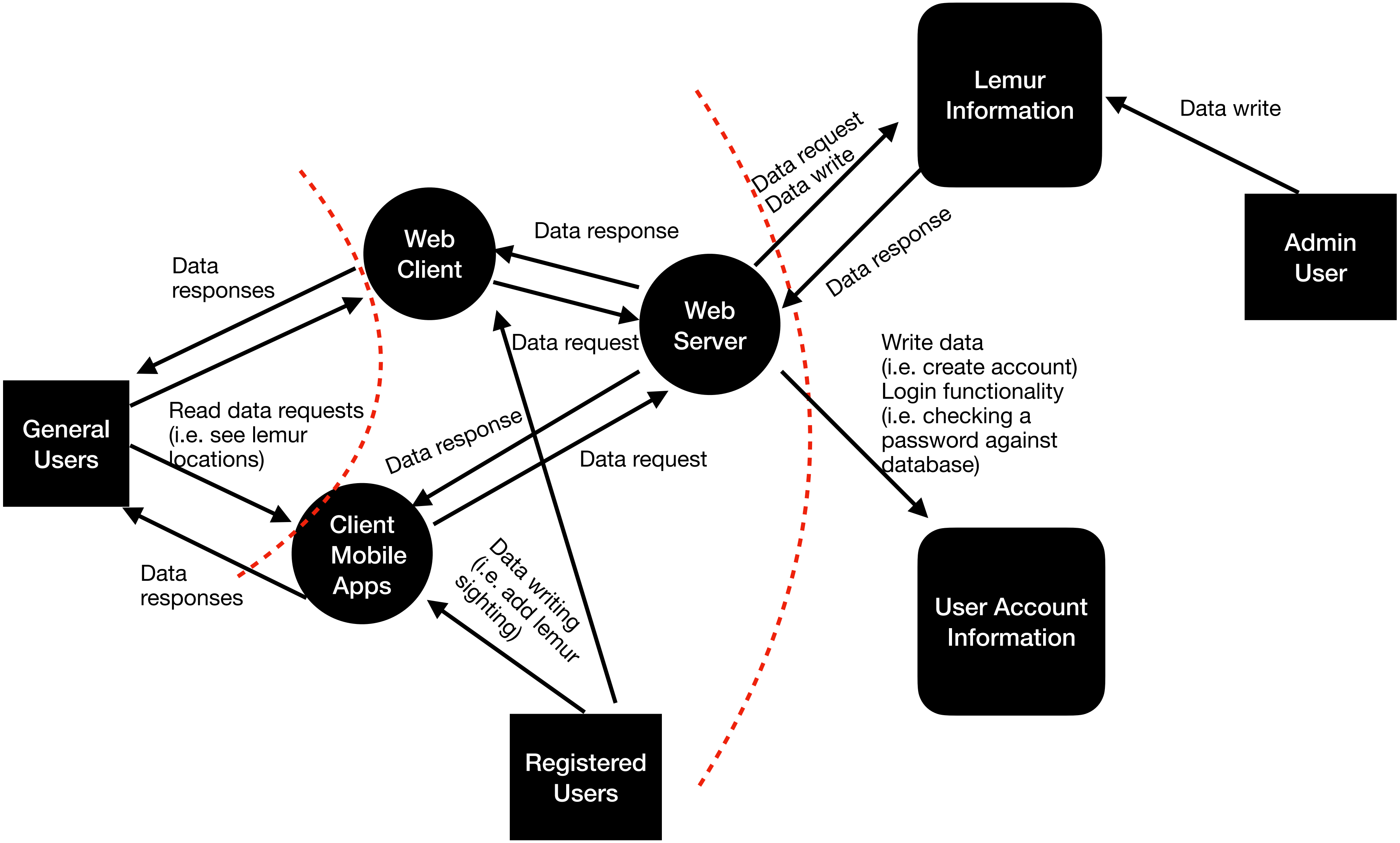
Lemur Information
Data write
Admin User
Data request
Data write
Data response
Web Client
Data response
Data responses
Web Server
Data request
General Users
Read data requests (i.e. see lemur locations)
Data response
Data request
Write data (i.e. create account) Login functionality (i.e. checking a password against database)
Client Mobile Apps
Data responses
Data writing (i.e. add lemur sighting)
User Account Information
Registered Users

List of threats to David’s Lemur Network:

Threat: User inputting false lemur sighting

Mitigation: Admin user is able to verify data by viewing (public) conversations and sightings, removing any data that may seem problematic.

STRIDE label: (T)ampering with data

Threat: SQL injection attacks into database

Mitigation: Only registered users are able to add data to the databases, allowing for admins to see if a user adds harmful data, along with measures to prevent users from adding data directly into database (aside from account creation which would have separate measures for SQL injection)

STRIDE label: (T)ampering with data, (R)epudiation

Threat: User being vulnerable to a lemur attack because they do not have access to the data

Mitigation: Login is only required to add entries, allowing anyone to view the lemur information without barrier.

STRIDE label: (D)enial of service

Threat: Gaining access to user account information

Mitigation: Encryption of data so that confidential information is not stored in plain text. Storing user information in a separate database that no one has read privileges to access.

STRIDE label: (I)nformation disclosure

Threat: ARP attack to control user's account so that one can enter false information. (The lemurs might try to thwart the integrity of the system!)

Mitigation: Requiring two-factor authentication when accessing account from a new device.

STRIDE label: (S)poofing

Threat: User may find and attempt to use a backdoor to create an entry without a registered account.

Mitigation: Require all entries to be linked to an account such that an entry without a connection to an account would be rejected by the system.

STRIDE label: (E)levation of privilege, (R)epudiation

Threat: User may be unable to add an entry due to being locked out of their account.

Mitigation: Upon creation of account, require users to submit security questions that may be used in the case they forget their password.

STRIDE label: (D)enial of service