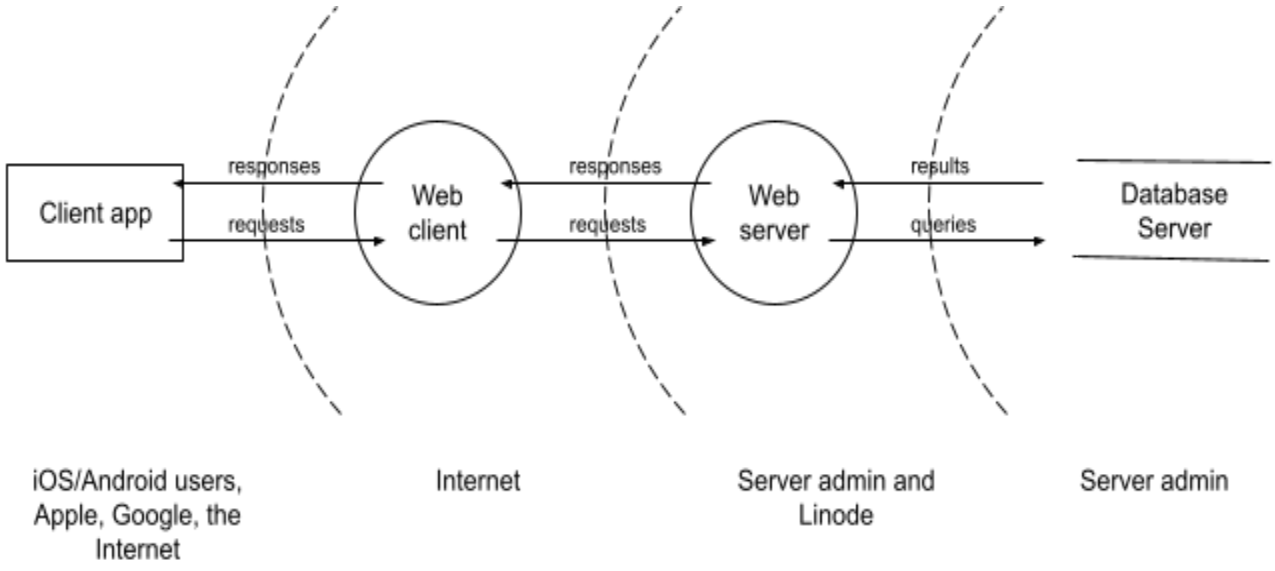
Brian Rhee and Avery Hall

Data Flow Diagram



Threats

- Spoofing
    - A user impersonating another user by finding their username and using it to log into their account
        - Mitigation: Requiring username and password in order to access user accounts
    - A user impersonates another user by creating an account that goes by the same name and drawing other users into devious tapir-scams.
        - Mitigation: Requiring unique usernames when registering accounts
    - A hacker has already compromised a user's email address associated with their Tapirs Unlimited account, and resets their password and takes control of their account using only their email
        - Additionally require answers to security questions in order to reset password
- Tampering *(Tapir-ing?)*
    - A malicious entity could intercept and change data after it leaves the client and before it reaches the server
        - Mitigation: Automatically using HMACs on data sent to the server
- Repudiation

    - TapirsUnlimited.com begins to sell T-Shirts and other merch, and receives a large order from one user whose credit card details are already saved in the site; however, the user later denies making the purchase in court
        - Mitigation: Require digital signatures for all client-server interactions in order to ensure non-repudiation in this sort of situation
    - A user denies leaving a hateful message on a forum page in court
        - Mitigation: Record time stamps of messages and compare to any records of outgoing packets on the host machine at the same time
- Information Disclosure
    - User password is intercepted in transit or its plaintext is stolen directly from the database server
        - Mitigation: A hashed version of the password is stored in the database server, which is compared with hashed versions of password attempts as the user attempts to login
    - Third party intercepts and reads privates messages exchanged between users
        - Mitigation: End-to-end encryption of messages using a combination of AES and RSA
- Denial of Service
    - Hackers orchestrate a DDOS attack on the Tapirs Unlimited server
        - Mitigation: Limit rates of website traffic to a certain amount, perhaps on an hourly basis and take prescribed measures if that limit is ever exceeded
    - A malicious, tapir-hating individual attempts to disrupt availability of Tapirs Unlimited by creating hundreds of spam accounts and flooding the server with fake traffic
        - Mitigation: Implement some combination of Captchas and two factor authentication when users attempt to sign up for an account or log in to a previously existing account
- Elevation of Privilege
    - A hacker tries to enact website changes by guessing the session ID (found in HTTP cookie) of an administrator
        - Mitigation: a) Make session ID's long, varied and difficult to guess, and b) add additional factors besides session ID to confirm and grant user privileges
    - A hacker uses an exploit made possible by a bug to enact changes with admin privileges, but these changes are hard to track and can result in serious damage in the time they take to spot
        - Mitigation: Audit and log all administrative activity for constant inspection and future reference