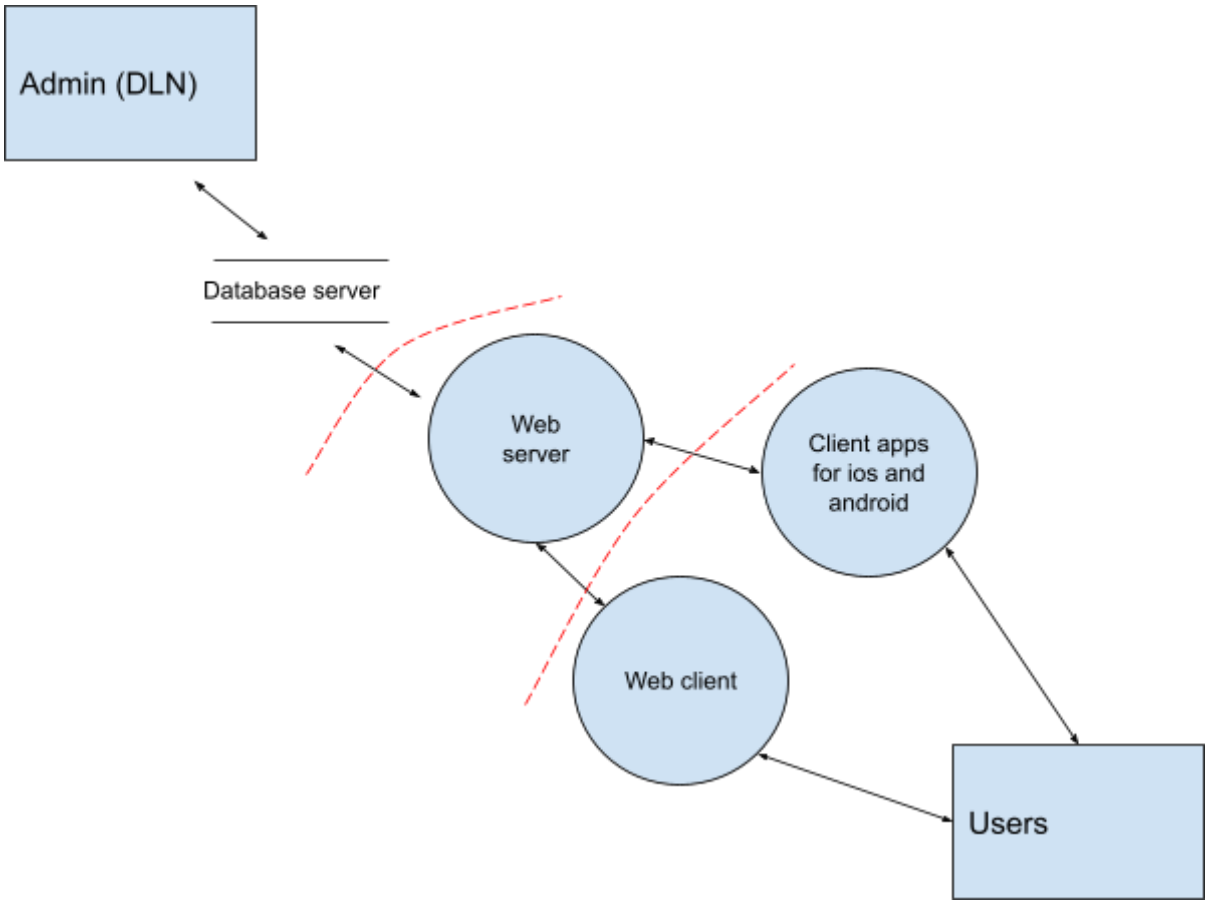
STRIDE Analysis of David Lemur Network (DLN)

Rebecca Fox and Yemi Shin

Data flow diagram:



Threats/Mitigations:

S (Spoofing) -

1. **Threat:** Someone might be able to impersonate a user or computer on the web server and gain access to sensitive information on the database server. For example, Yemi logging into Rebecca's DLN and accessing her credit card information/address.
    a. **Mitigation:** Dual authentication, HTTPS, access control logs
2. **Threat:** Fake client apps (that impersonate the real client apps) that appear to be securely connecting to the system but are instead malicious. For example, a fake "DLN" might pretend to be the real one, gaining access to the user's credentials.

    a. **Mitigation:** Require the verification of the certificates of the ios, android, and web clients prior to engaging in TLS/HTTPS

T (Tampering with data) -

1. **Threat:** A person impersonating admin could directly tamper with the data (for example by stealing the pw of the admin).
    a. **Mitigation:** Admin authentication (IPSec authentication), dual authentication, TLS/HTTPS protocol, access control logs (filter network interactions, and only allow packets to flow from source to destination)

R (Repudiation) -

1. **Threat:** An attacker can go into the database and delete or modify any usage logs or access control logs which would make it so that no one can track the actions of any one user, including the attacker.
    a. **Mitigation:** Keep everything encrypted and hashed so that an attacker cannot read or covertly modify the information.

I (Information Disclosure) -

1. **Threat:** Malicious users could be able to eavesdrop on the messages passed between the database server and the web server.
    a. **Mitigation:** All interactions occur on HTTPS.

D (Denial of Service) -

1. **Threat:** A malicious person could gain access to the web client and block all information between the web server and the web client, causing valid users to be unable to see information on the web client
    a. **Mitigation:** Utilize HTTPS/TLS to prevent Mal from gaining access to network messages in the first place.
2. **Threat:** Distributed Denial of Service - a malicious user could bombard the web / ios / android client and cause enormous traffic, which would overload the web server
    a. **Mitigation:** Access control logs, monitoring and filtering traffic on web server

E (Elevation of privilege) -

1. **Threat:** A malicious person could elevate their security level to admin, and alter the database.

a. **Mitigation:** Admin authentication(IPSec authentication), access control logs, TLS/HTTPS protocol