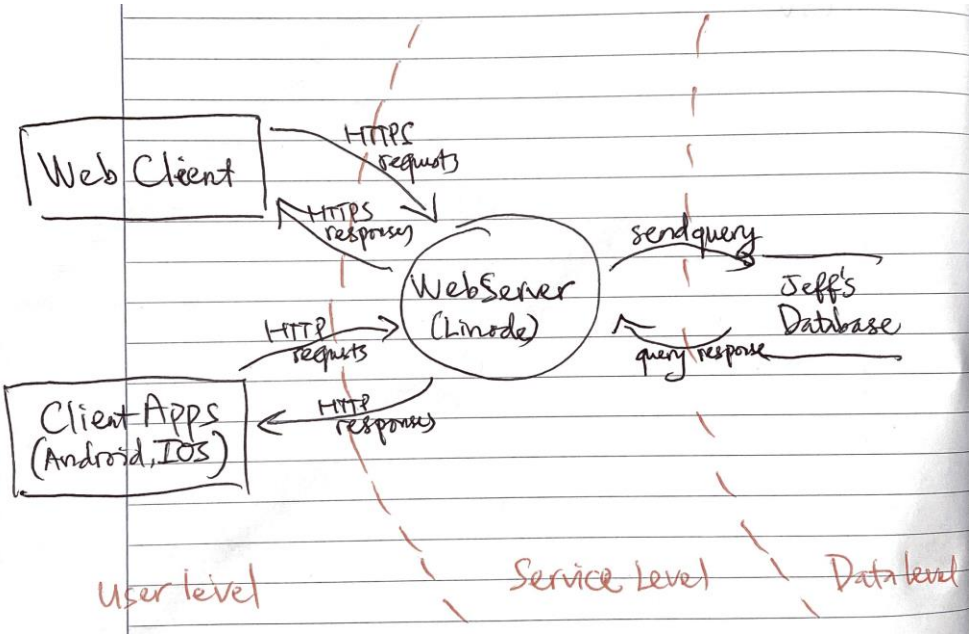
Minh Pham

Data Flow Diagram



STRIDE

We will use Mal to refer to the person that performs attacks and malicious activities

---- **Spoofing** ----

Threat 1: Mal sends users phishing emails, saying someone logged into your account, follow this link to block the person, or any similar kinds, that prompts users to enter credentials.

Mitigations: Make it a public rule that our website never sends out emails.

Threat 2: Mal contacts users directly, disguising as the website staff, to get credentials out of users

Mitigations: Raise awareness to users to know that no staff will reach out asking for credentials.

---- **Tampering** ----

Threat 1: Mal uses any kinds of forms to attempt SQL injection to tamper with the database from Jeff's machine

Mitigations: Use techniques such as input validation, parametrized queries, stored procedures in the API to query from the database.

---- **Repudiation** ----

Threat 1: Mal performs malicious activities on the website to scam people then delete the trace of activities and hold no responsibilities.

Mitigations: Keep in the database all activities of users for a period of time even if they are deleted in public.

---- **Information Disclosure** ----

Threat 1: Mal performs SQL injection in a form to query private data.

Mitigations: Use techniques such as input validation, parametrized queries, stored procedures in the API to query from the database.

Threat 2: Mal acts as Eve and eavesdrops on user's network reads user's interaction with the TU web server.

Mitigations: Make all interactions with the TU server occur over HTTPS so that Eve cannot read anything.

Threat 3: Mal guesses user's password and logs into user's account.

Mitigations: Require users to use complicated passwords and set up security questions.

---- **Denial of Service** ----

Threat 1: Mal breaks into Jeff's office and deletes a user from the database. That user can no longer use their account/

Mitigations: Jeff needs to install in real life security measures.

Threat 2: If there's a public API of the website, Mal can spam requests to throttle legit ones from real users.

Mitigations: Set a time limit on how fast one can send requests using that public API

Threat 3: Similar to threat 2, now Mal just directly uses the website frontend to send requests

Mitigations: Set a time limit on how fast one can post or get information, limit on how many words per post/comment, etc..

---- **Elevation of Privilege** ----

Threat 1: If the website has admin roles, Mal can target that admin person in real life to get their credentials

Mitigations: Avoid giving too much power to certain types of accounts

Threat 2: Mal performs Source IP spoofing (https://www.internetsociety.org/resources/doc/2015/addressing-the-challenge-of-ip-spoofing/) to send data accross traffics and acts as if they are users. They elevated their privilege to be a specific person.

Mitigations: According to the articles, there are a few ways: Ingress filtering described in BCP38, or Unicast Reverse Path Forwarding, or uRPF.