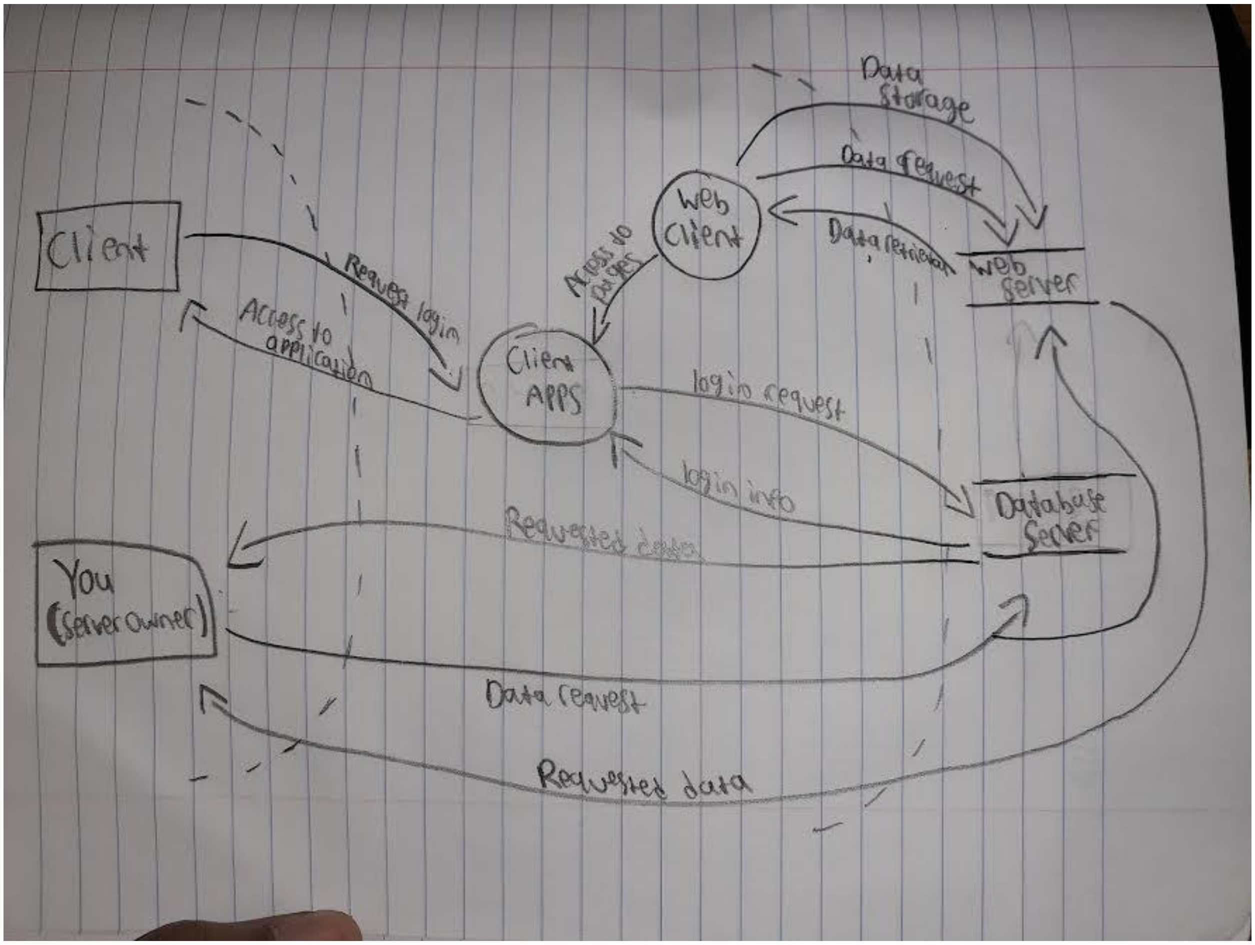
Devin Lewis | CS 338



STRIDE Threats

Spoofing:

- A person enters your home with the malicious intent to mess up your database server
  Mitigations: Still require your own username and password, the web server is owned by someone else.

Tampering:

- A user has gained Linode admin access and intends to manipulate the web server
  Mitigations: The data is actually held on the database server, communications with other clients is through HTTPS

Repudiation:

- A trickster intends to troll on the various chat logs with a spoofed account
  Mitigations: The server for communication is monitored by Linode (I think)

Information disclosure:

- Eve intends to eavesdrop on the database server port and wait for it to transfer account information to its clients
  Mitigations: The communication between server and Client is through HTTPS

Denial of service:

- Someone breaks into your house and smashes your computer with the server on it
  Mitigations: You locked your door and windows, the computer is stored in a locked room, guard dog?

Elevation of privilege:

- A maleficent vagrant access Linode administrator authentication to try and obtain unreleased high quality tapir pictures
  Mitigations: The picture data is located on the database server requiring HTTPS communication between the database and web servers.