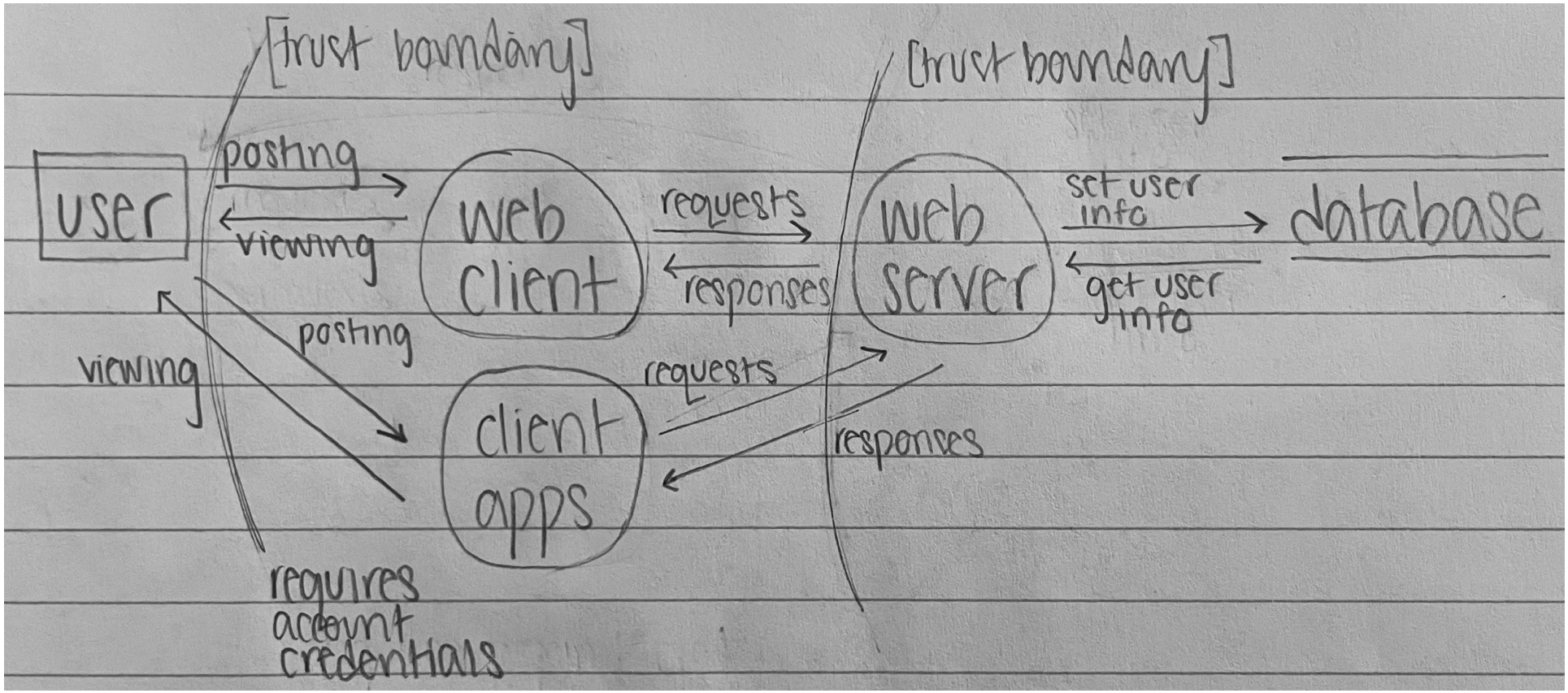
Lane Maitland

STRIDE	**violates…**	**example: threat**	**example: mitigation**
spoofing	authentication	- I know that Jeff has an account, so I try to guess his username/password to gain control. - I gather a large list of email addresses connected to accounts, and I send them fake updates about TU from a fake company account. (I may advertise fake premium features and say that users must pay a monthly fee to access them.)	- do not tell people what programs you have created accounts for - use different/intricate usernames/passwords so that they are more difficult for others to guess correctly - connect different/private email address to account in case someone tries to reset your password and already has access to another of your email accounts - ensure user email addresses are not public (in other words, their username is not just their email address)
tampering	integrity	- I gain access to the database and add fake facts about tapirs to users' accounts. - I prevent the web server from loading photos and videos.	- require username/password (or other authentication) to access database and web server
repudiation	non-repudiation	- I create an account, choose not to connect it to my email, and message people to say that they qualify for a verified account. Since I did not connect my email, no one knows who controls the account, so they cannot prevent me from creating multiple accounts with this purpose. - I work for Jeff, so he grants me access to all TU data and processes. When changes appear, he does not know which employee is responsible for them.	- require email address to create account, even if email is not displayed publicly - provide employees with company accounts to track their contributions, and ensure that employees only have access to data/processes pertaining to their position
information disclosure	confidentiality	- I search for any user, and I can easily see all of their activity/posts. - I can see when any user is active on their account by checking their status.	- allow users to create private accounts, which requires them to accept requests of other user accounts and prevents their account activity/posts from being visible to anyone - allow users to disable their status
denial of service	availability	- I spam the chat so that other users cannot post. - I gain control of the ports 80 and 443, and I prevent any TU process from running.	- enforce limit on frequency of posts - require username/password (or other authentication) to access ports of web server
elevation of privilege	authorization	- I work for Jeff, so he grants me access to all TU data and processes. I abuse this by documenting users' credit card information for my personal use. - I want another user's username, so I report their account. The account is immediately banned, and the username becomes available to me.	- restrict what employees can access - require investigation before banning reported accounts


[trust boundary]
[trust boundary]
user
posting
viewing
web client
requests
responses
web server
set user info
get user info
database
viewing
posting
client apps
requests
responses
requires account credentials