Author: Robbie Young

Spoofing (S):

- Bruce Schneier could impersonate and imitate the web client and/or client apps, such that any user that enters any information could be received by Bruce. Mitigation would be to use certificates.
- Bruce could impersonate Linode using similar tactics, this time being able to monitor any data coming in and out. Mitigation would again be to use certificates.
-

Tampering (T):

- Bruce could try and modify any data stored in the database, such as a user's username, password, address, or worst-case scenario delete Tapirs photos! Mitigation would be to use hashes of each photo to help file integrity.

Repudiation (R):

- Bruce could act as an intermediatory between the server and the user, such that Tapirs Unlimited would be unable to prove that Bruce was involved. Mitigation would be certificates to prevent this in the first place.

Information on Disclosure (I):

- Bruce could act as Eve, and spy on people either in real life or by impersonating (as explained in spoofing), such that Bruce is now able to read anything that is being transmitted (it may not be able to read if send in HTTPS however). There is not much to stop the HTTP transmission from being read, however using encryption (HTTPS) does prevent this as mitigation.

Denial of Service (D):

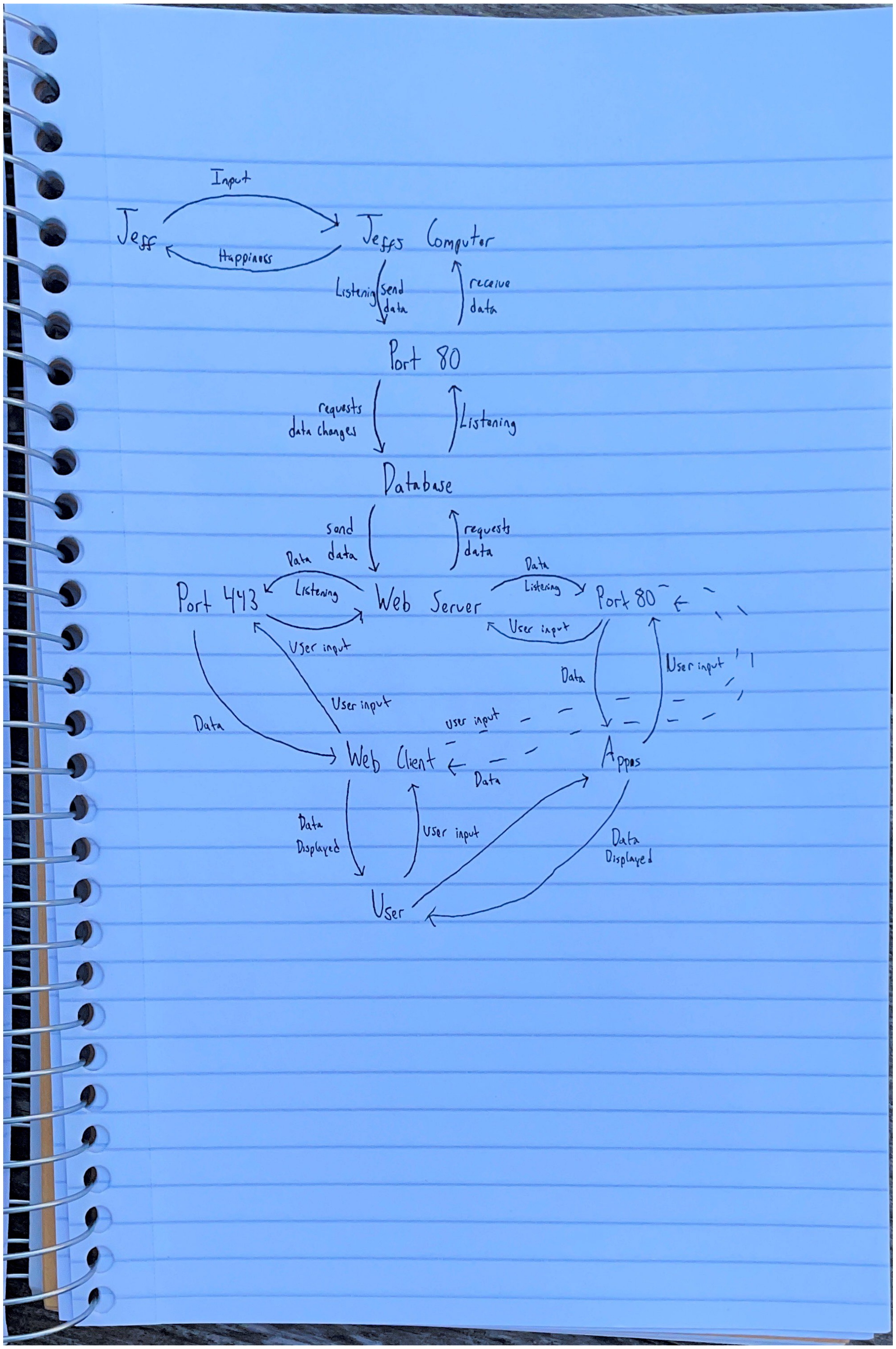
- Bruce could nuke the entire world. Mitigation is no nukes!
- Bruce could launch a DDOS attack on the web server itself through either the WC or the CA or on any user. Mitigation could be to have limits on how many requests per minute or to get a better web server.
- Bruce could physically render any computers in this operation inoperable (web server or any user again). Mitigation would be to hire many many bodyguards.

Elevation of Privilege (E):

- Bruce could steal Jeff's identity and log on to his computer, allowing him to modify any data in the database. Mitigation would be for Jeff to hold on to his SSN and credit card info.
- Bruce could buy Linode and grant himself access to the web server, allowing to listen onto any data transmission between user and server. Mitigation would be to bankrupt Bruce.
- Bruce could become a user himself, allowing him to view his own name, address, location, and as many Taphir photos as he wants! Mitigation is to ban Bruce.

(Sorry Bruce no hate I really enjoyed your talk <3)

(sorry for the dotted lines between the web client and port 80, I realized a little too late)


Input
Jeff
Jeffs Computer
Happiness
Listening
send data
receive data
Port 80
requests data changes
Listening
Database
send data
requests data
Data
Listening
Port 443
Web Server
User input
Data
Listening
Port 80
User input
Data
User input
User input
Data
user input
Web Client
Data
Apps
Data Displayed
User input
Data Displayed
User