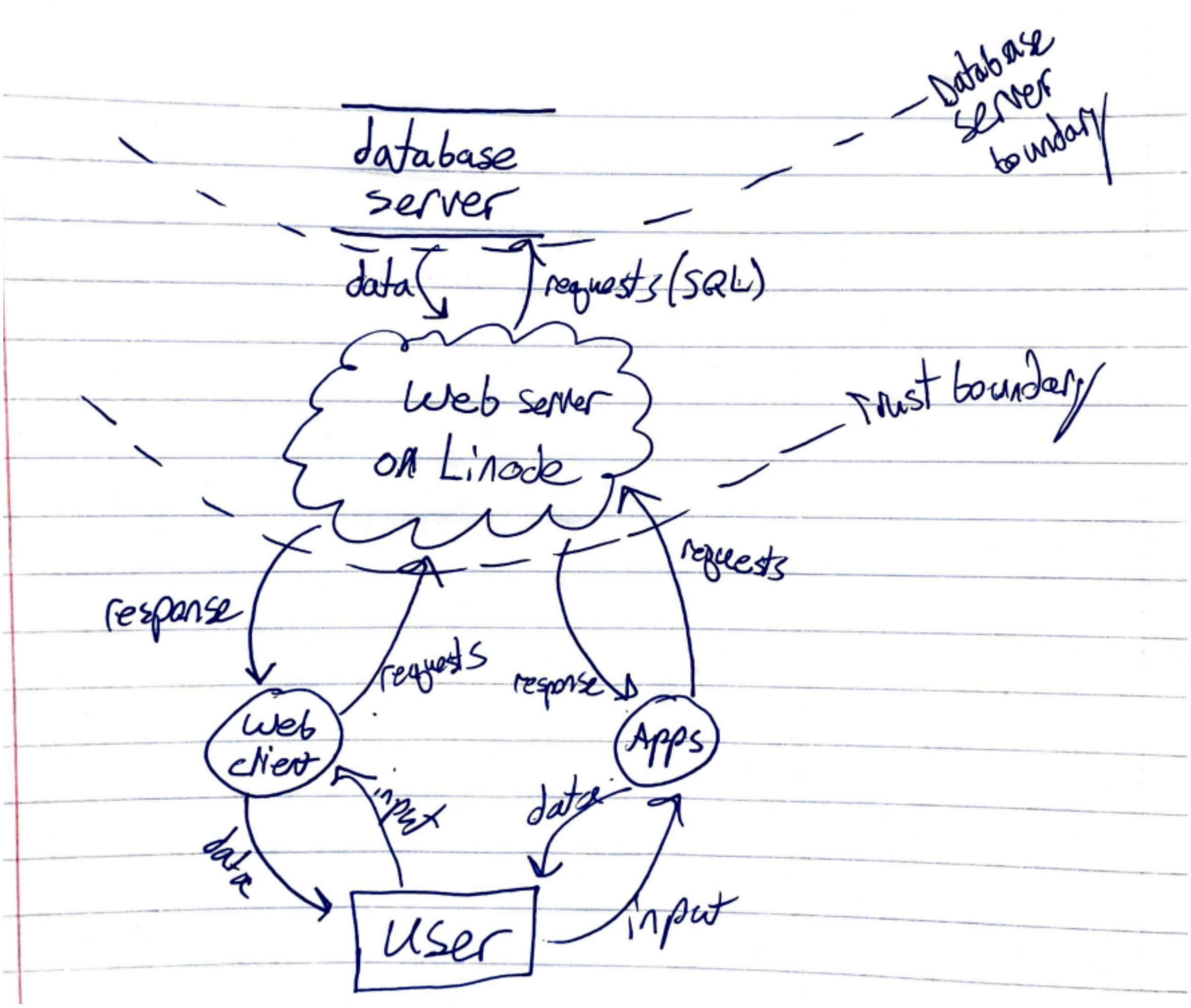
Threat Analysis Using STRIDE
Alex Falk

Data flow diagram



STRIDE
- Spoofing
    - Attacker spoofs a known user’s IP address try to gain access to their account
        - Require 2 factor authentication for account access
    - Attacker steals login credentials and turns stolen accounts into bot accounts
        - Look for and remove posts that appear to be phishing in some way
- Tampering
    - Attacker interferes with communication between the database and the web server. The original request asks for tapir pictures but gets changed to ask for credit card information.
        - Require challenges from the database for sensitive information

- Repudiation
    - Attacker gains access to an account and using these credentials makes a change to the user's information in the database. The database logs this change as being performed by the username associated with the account.
        - When logging changes in the database, use the user's IP address. Cross reference the IP addresses to check whether the information has been edited by an IP address associated with the account.
    - Attacker creates an account and posts things that go against TU's TOS or are illegal
        - Require a valid phone number to be used during account set up. Also, store IP addresses when creating accounts
- Information disclosure
    - Attacker performs SQL injection trying to get unauthorized access to information in the database
        - Use parametrized queries
    - Attacker gains access to database
        - Encrypt data/use hashes to store password information
- Denial of service
    - Attacker performs denial of service attack on Linode
        - Set packet/query limit for IP addresses (helps with DoS more than DDos)
    - Attacker spams TU with thousands of posts
        - Suspend accounts that post too much (should be a pattern of many similar posts, posts too quickly)
- Elevation of privilege
    - Attacker wants to access a user's private Tapir videos by using their account
        - Require strong password parameters (special symbols, numbers, no names, etc.)