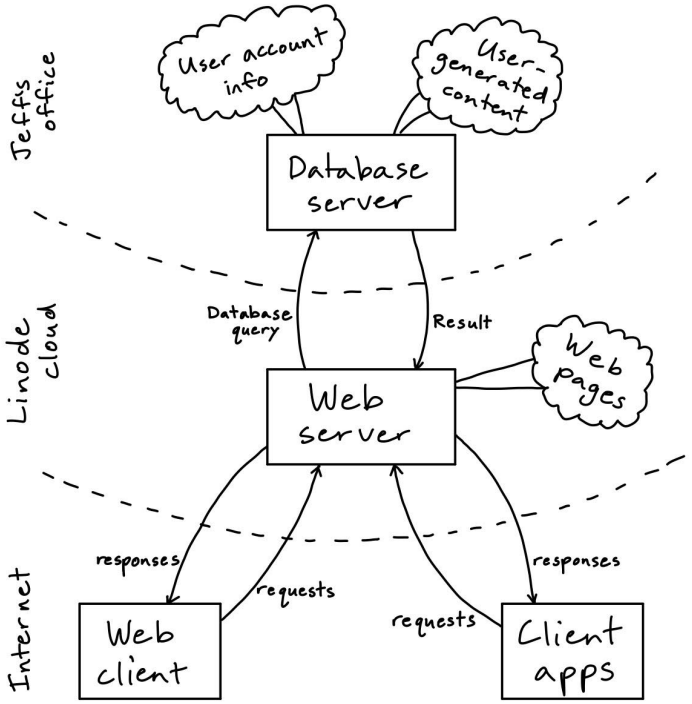
McKenna Wirth and Antonia Ritter
CS338 Spring 2022

THREAT ANALYSIS USING STRIDE

Data Flow Diagram



Threats and Mitigations

Spoofing:

- As of 5:00pm on 05.04.22, tapirsunlimited.com does **not** have a valid certificate, making it easier for someone to impersonate the web server.
    - Mitigation: get an updated certificate from a certificate authority.
    - Update: this has since been fixed with a valid certificate from Let's Encrypt, as of 8:00pm on 05.04.22.
- Someone setting up tapirslimited.com and charging for the service.
    - Mitigation: make sure tapir fans know the real url, perhaps by advertising or social media, possibly in collaboration with zoos.

Tampering (or tapirs):

- Changing data stored in the database server via remote access.

    - Mitigation: adding access requirements to only allow authorized requests or physical access.
- Intercepting and altering data sent to/from the database server from the web server OR from the web server to/from a client.
    - Mitigation: using HTTPS to encrypt these communications with an encryption method that prevents PITM attacks.

Repudiation:

- Tapirs Unlimited users creating and using anonymous throw-away accounts to post inflammatory or offensive content that is not tied to their identity.
    - Mitigation: requiring accounts to be a certain age before allowing them to make posts, or requiring users to provide additional identification when creating an account and not allowing multiple accounts with the same identification information.
- Someone charging tapir figurine purchases to another user's account.
    - Mitigation: dual authentication on accounts, and/or extra verification required to make purchases.

Information disclosure:

- Eavesdropping on communication between clients and web server.
    - Mitigation: Use HTTPS instead of HTTP website templates.
- Publishing the IP address from which they access the site.
    - Mitigation: only storing this information for a limited time and storing it as a hash with salt.
- Releasing credit card or password information.
    - Mitigation: store this information in the database server as hashes.

Denial of service:

- A hack that takes the web server offline, for instance using a SYN flood.
    - Mitigation: have backups of the servers.
- Banning a user.
    - Mitigation: to be honest, this is a feature not a bug, as long as its an administrator banning them.

Elevation of privilege:

- Giving an account mod privileges (in chat rooms, for example).
    - Mitigation: require verification by another mod before changing an account's privileges.
- Deleting someone else's posts.

    - Mitigation: require password verification or approval by a moderator.

Other:

- Someone could break into Jeff's home office while he's at the coffee shop at 7am and steal, damage, or add a program that can mess with the database server. This fits in multiple STRIDE categories:
    - Tampering- if data are modified.
    - Repudiation- unless they are caught or leave behind a message, there is no way to know who did it.
    - Mitigation: increasing physical security of the database server by locking the office and having backups.
- Users could impersonate other users, either by creating similar account names or by logging into others' accounts. This fits in all of the STRIDE categories:
    - Spoofing- it involves impersonation.
    - Tampering- by changing information.
    - Repudiation- in that your actions are not tied to you.
    - Information disclosure- when viewing user-only pages like the public profile.
    - Denial of service- if the password is changed or they are otherwise prevented from using their account.
    - Elevation of privilege- because you're accessing an account you shouldn't have access to.
    - Mitigation: restricting usernames to avoid extremely similar usernames, requiring dual authentication for logging on.
- Scammers/scammer bots sending malicious links.
    - Mitigation: have users report suspicious activity and/or auto-ban accounts with suspicious (particularly bot-like) behavior.