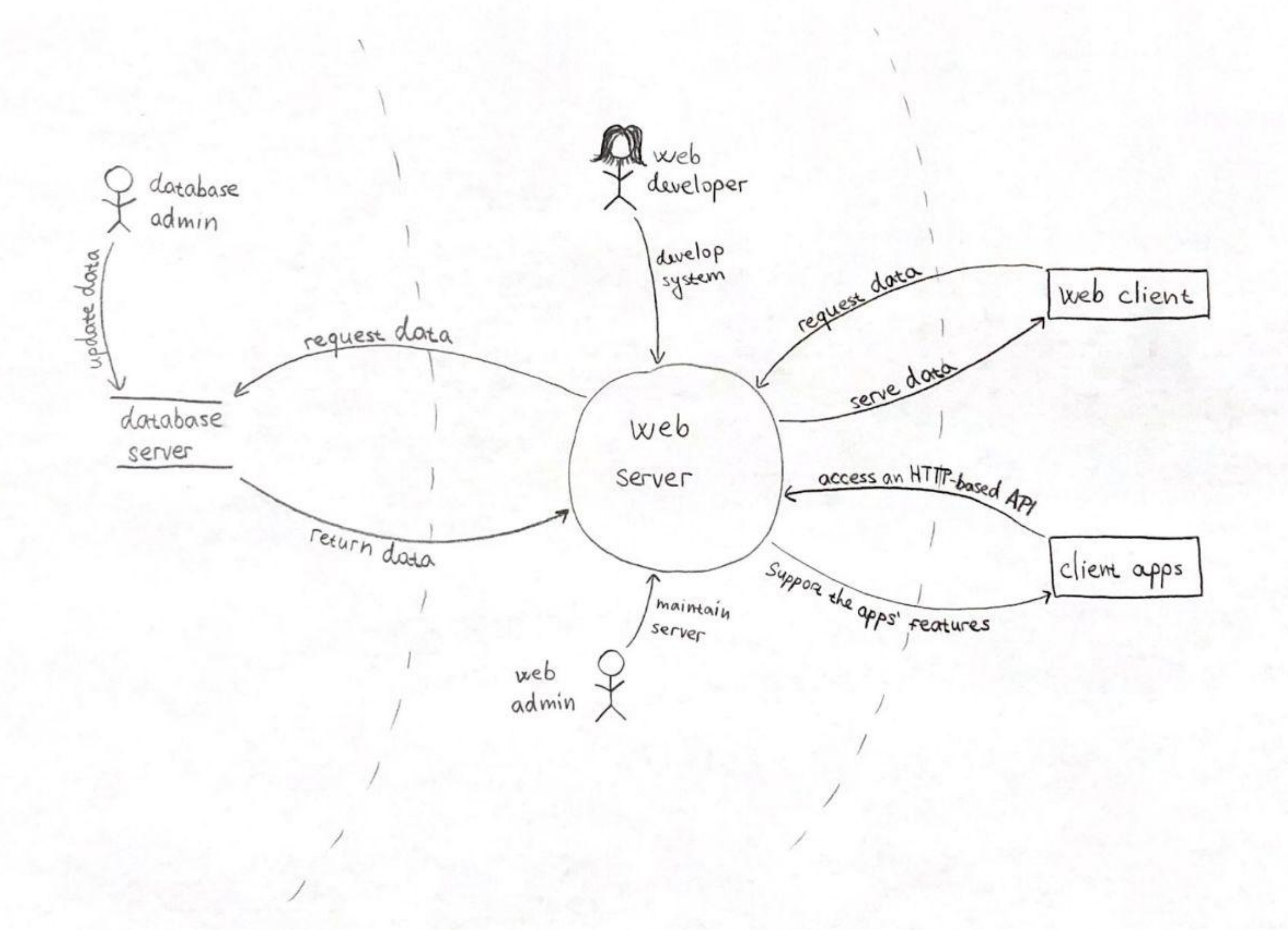
Adela Dujsikova & Ethan Li
CS 231
Professor Jeff Ondich
May 3rd, 2021

STRIDE Assignment

Data Flow Diagram:



List of potential threats and corresponding mitigations:

- Eavesdropper on user's network reads user's interaction with the DLN web server (example)
    - Mitigation: all interactions with the DLN server occur over HTTPS
    - Element(s) of STRIDE: information disclosure

- Eavesdropping communication between web server and the database server
    - Mitigation: all interactions with the DLN server occur over HTTPS
    - Element(s) of STRIDE: information disclosure

- ARP poisoning of the Web Server
    - Mitigation: clients using VPN, static ARP entries in the server, using detection tools such as XArp
    - Element(s) of STRIDE: spoofing, information disclosure

- Unauthorized access to database from a client account, potentially changing data
    - Mitigation: Block all connection to the database besides the Web Server and database admin; require digital signatures for admin login
    - Element(s) of STRIDE: information disclosure, tampering

- Unauthorized database admin login
    - Mitigation: Ensure redundancies in admin login credential protection (no writing password down on a piece of paper and sticking it on the computer, must use long and complicated passwords)
    - Element(s) of STRIDE: elevation of privilege, repudiation, information disclosure, spoofing, (potentially) tampering and denial of service

- Unauthorized web developer login
    - Mitigation: Ensure redundancies in admin login credential protection (no writing password down on a piece of paper and sticking it on the computer, must use long and complicated passwords)
    - Element(s) of STRIDE: elevation of privilege, repudiation, information disclosure, spoofing, (potentially) denial of service

- HTTP flood DDoS
    - Mitigation: web application firewall
    - Element(s) of STRIDE: denial of service

- SYN flood DDoS
    - Mitigation: firewalls and IPS devices
    - Element(s) of STRIDE: denial of service

- Fake accounts / bot accounts affecting lemur database accuracy
    - Mitigation: Account creation verification processes (eg. CAPTCHA) and human monitor and inspection of suspicious account activities; restrict

lemur data reporting to users within a certain radius of Northfield, MN, USA.

  - Element(s) of STRIDE: repudiation, denial of service (when the database is flooded by inaccurate bot account inputs)

- Physical damage to or destruction of database server
  - Mitigation: Protect the database at an undisclosed location
  - Element(s) of STRIDE: denial of service, tampering

- Web developer includes a bug on the system that allows an attacker to access the database (the attacker and web developer are on the same team)
  - Mitigation: review of the code by multiple web developers
  - Element(s) of STRIDE: information disclosure, possibly tampering

- Web admin changes a client privileges from “Amateur Lemur Spotter” to “Professional Lemurist”
  - Mitigation: all actions of web admins would be watched and documented
  - Element(s) of STRIDE: elevation of privilege

- Person-in-the-middle attack on the messages between clients
  - Mitigation: HTTPS, hashing, encrypting
  - Element(s) of STRIDE: information disclosure, spoofing, could be tampering, denial of service (if the attacker doesn’t forward the message or pretends the server is unavailable)

- Unauthorized client login due to a phishing attack
  - Mitigation: server blocks logins from suspicious locations and checks with the client whether it is actually them; 2 factor authentication
  - Element(s) of STRIDE: spoofing, tampering, repudiation, information disclosure, denial of service (if the attacker changes the password)

- False or irrelevant data input from client accounts
  - Mitigation: Content control by database admin and account suspension by web admin.
  - Element(s) of STRIDE: denial of service (it’s a bit of a stretch but it’s the best category of STRIDE to fit in)

- Replay attack between either the web server and clients or between web server and database
  - Mitigation: Using time-sensitive digital signature; using idempotency tokens

- Element(s) of STRIDE: tampering, repudiation