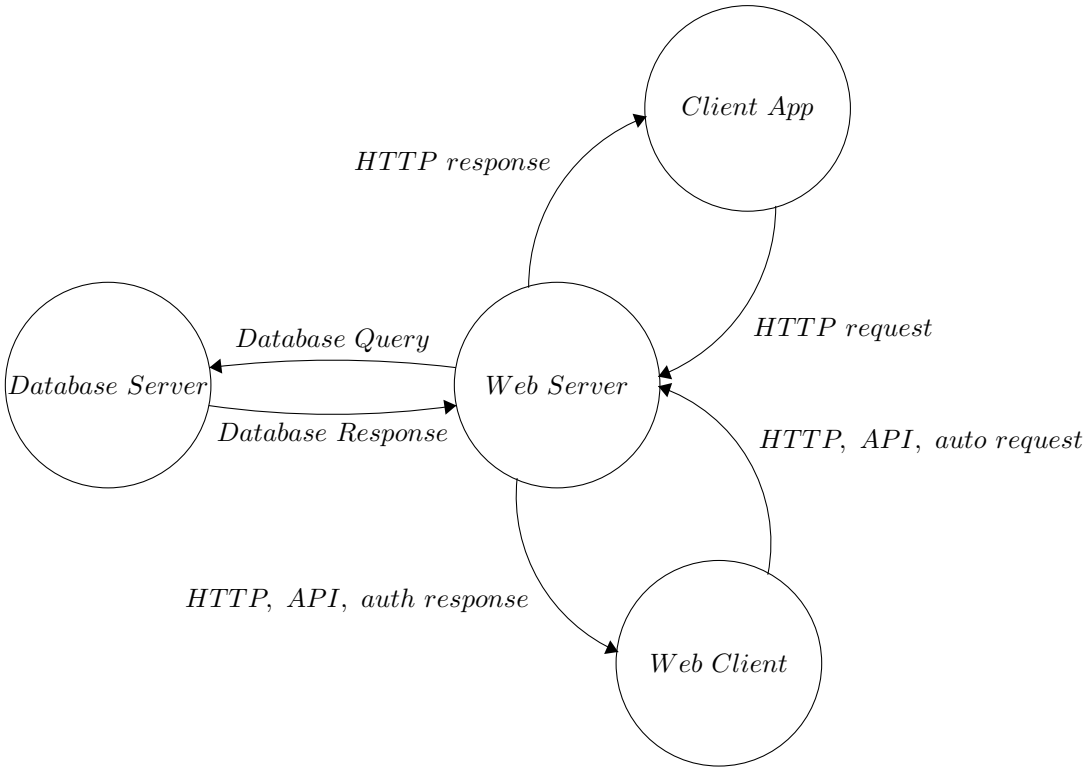
CS338 Threat Analysis with STRIDE

Kuo Wang

April 2022

1 Data Flow Diagram



2 STRIDE analysis

1. PiTM attack in communication between app and web server, or between database server and web server. As a result, data is manipulated by and leaked to an unauthorized personnel.
    - STRIDE characteristics: Spoofing, Tampering, Integrity, Elevation of privilege
    - Fix: use HTTPS with certificate and signature system in the communications. Also do end-to-end encryption on the communicated data.
2. DDoS attack against the web server or database server
    - STRIDE characteristics: Denial of service
    - fix: use firewalls on the two servers
3. Someone can query data from the database and manipulate sensitive information like passwords
    - STRIDE characteristics: Spoofing, Tampering, Information Disclosure, Elevation of privilege
    - fix: Secure hash the passwords; end-to-end encrypt all data; requiring authentication in database requests
4. Someone breaks into Jeff's home and steals the hard drive. All data including passwords are stolen.
    - STRIDE characteristics: Information disclosure
    - fix: implement server-side encryption so all data on the hard drive are encrypted; install good locks and security systems to secure server parameter
5. Someone attacks Linode or it bugs out. Web server is down from service.
    - STRIDE characteristics: Denial of service
    - fix: Have redundant server elsewhere as a plan-B.
6. Jeff's home office experiences a network server interruption or man-made/natural disaster
    - STRIDE characteristics: Denial of service
    - fix: have regular back-up of data elsewhere (hard drive in safe location or cloud archive services)
7. Someone gets ahold of Jeff's admin account, and wrecks havoc on the file and permissions system
    - STRIDE characteristics: Elevation of Privilege, Information Disclosure, Tampering
    - fix: safeguard admin and root password, use MFA for added security, and reguarly change password
8. Someone gets ahold of Jeff's admin account, elevates privilege of another account, and uses that account maliciously while erasing all activity logs
    - STRIDE characteristics: Elevation of Privilege, Repudiation, Information Disclosure, Tampering
    - fix: In addition to procedures like in 7, implement immediate alert (like via phone messaging) when someone exercises high privileged actions on the servers, or when a new high-privileged role is assigned