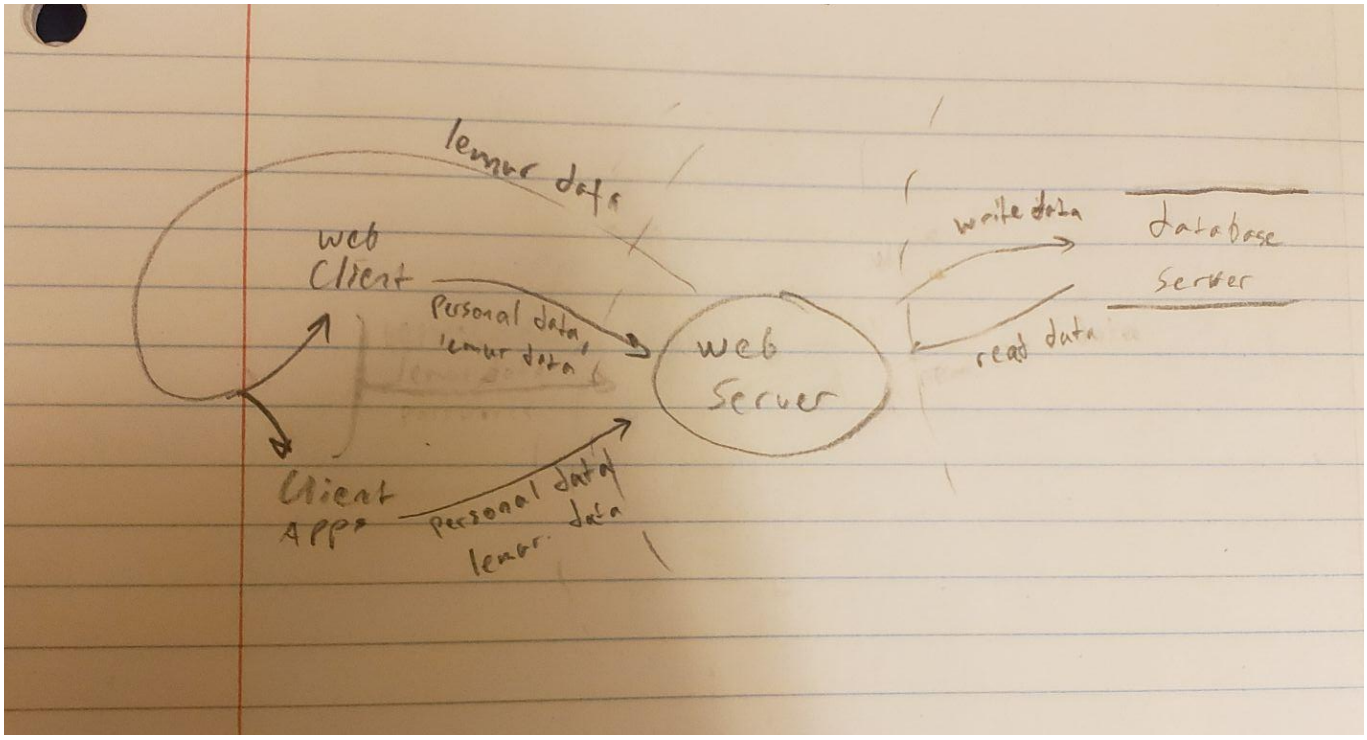
Authors: Anders Shenholm Riaz Kelly

STRIDE Analysis of DLN



1. An attacker could overload the web server with automated login attempts (D). Mitigation: Add a captcha to slow down computers logging into the server.
2. An attacker could use established accounts to overload the database server with automated lemur reports (D). Mitigation: disable accounts that are creating an inhuman amount of lemur sightings. (give a generous amount of room for dedicated users but draw a line where activity gets totally implausible.)
3. An attacker could hit essential server hardware with a bat (D). Mitigation: keep the location of the server secret and physically secure it in a place that can't be entered without authentication.
4. An attacker could get the credentials to an admin account and mess with user chat, ban people, etc. (E). Mitigation: use a sort of duo authentication that requires confirmation from the admin's account in a different service which uses different credentials.
5. An attacker could eavesdrop on interactions between the web server and database server (I). Mitigation: use Public-key encryption for this interaction
6. A person in the middle could modify messages between web server and client (T). Mitigation: Send messages with signatures based on a known hash function so that client and server can ensure they're seeing the original message.

7. An attacker could impersonate the web server via ARP spoofing (S). Mitigation: send every message from the web server with a signature that the attacker can't recreate w/o the web server's private key.
8. An attacker could try to claim that an account (their account) didn't perform certain actions on the site (R). Mitigation: log user activity and back up data.
9. An attacker could try planting a faulty link for DLN that would occur in search results (S). Mitigation: use a simple, memorable URL or at least one that you emphasize in communication with users.
10. An attacker could impersonate DLN and send an email with a faulty link for DLN via email (S). Mitigation: don't send links to users, at most send plaintext urls which users can put in the search bar themselves.
11. An attacker could make inaccurate postings using someone else's account if they have access to their signed-in device (S/E). Mitigation: put an inactivity timer on connections to the server to minimize time where an AFK user's device will be available for attack.