Kaeden Berg and Kitty Tyree

- Spoofing
    - Creating new accounts with false identities
        - Allow only account per email
        - Implement a user report system, so people may report false user profiles.
        - Implement a verification system, there's a process to become verified on the network so other users know you are legitimately who you say
    - Password guessing algorithms
        - Limit the amount of guesses allowed before your ip is temporarily blocked. (Was previously lock accounts, see Denial of Service 2)
        - Limit the number of different accounts you can try passwords for before your ip is temporarily blocked.
    - Passwords seen from requests, or from malicious internal actors
        - Use an input-sensitive and preimage resistant hash function to hash passwords, and hash passwords immediately as the user types them, do not store the pre-hashed password once it has been hashed. Compare the hashes, not the plaintext passwords.
- Tampering
    - Modifying chats between users
        - Having encrypted communication with automatic Message Authentication Codes, ideally using public and private keys for the users to authenticate their messages.
    - A user changes other user's images/videos, captions, or location data.
        - Users can only change their own posts, location data is automatic (opt in) so users can't make false reports.
        - Changes can only be made to the database from the server, using approved client APIs.
    - A user intercepts or modifies requests
        - All requests and responses are done using HTTPS, so requests are encrypted safely.
- Repudiation
    - Attacks from unknown source
        - Keep an activity log (timecodes for when a user logs in or out, keep track of all requests made as they are made)
            - Provide a security agreement, we won't sell their data.
    - Attacker deletes account data
        - Keep activity log or a short period after account deletions
    - Internal attacker deletes or changes data
        - Admin changes are done through an api which also keeps an activity log associated with each account. Only admins may change the database.
- Information Disclosure
    - Attacker gains access to stored credit cards on the database
        - Don't store credit card information, allow paypal, or force users to enter in credit card information for each purchase, never store it in the database.

        - Credit card information is encrypted, only decrypted for purchases, and the credit card data is only viewable by system processes.
    - Attacker gains private information from chats
        - Chats are symmetrically encrypted between users, with a shared secret key agreed upon using PKI, or some internal version of that.
    - Attackers find addresses through location data
        - Location data could be anonymous for maps
        - Location data may be “fuzzied”, so the lemur spotting is nearby, not exact
        - Location data is only viewable on the post it is on, you can’t view every post for a specific user on a map.
        - Location data can be opted out
- Denial of Service
    - DDOS Botnet Attacks
        - Limit bot usage with Captcha
        - Only those with accounts can view the website/app
            - Make the service cost 1$ to make an account, to deter bots.
                - Card can’t pay for multiple accounts
        - Increase server capacity to handle large use spikes
    - Attackers lock every account by guessing generic passwords for every user
        - Instead of locking accounts from guesses, ban ip addresses
- Elevation of Privilege
    - Attacker obtains login credentials for an admin
        - Dual Authentication for privileged admin accounts
    - Attacker becomes a new admin
        - New admins have their identities verified, and are watched by trusted admins
    - Attackers change account privileges
        - User accounts can’t access administrator functions or become administrator accounts.
            - Admins get new accounts
            - Store a list of admin accounts that the system uses to verify account IDs with administrator level requests
                - Account IDs are hidden and hashed, similar to password comparisons.

Kaeden Berg and
Kitty Tyree