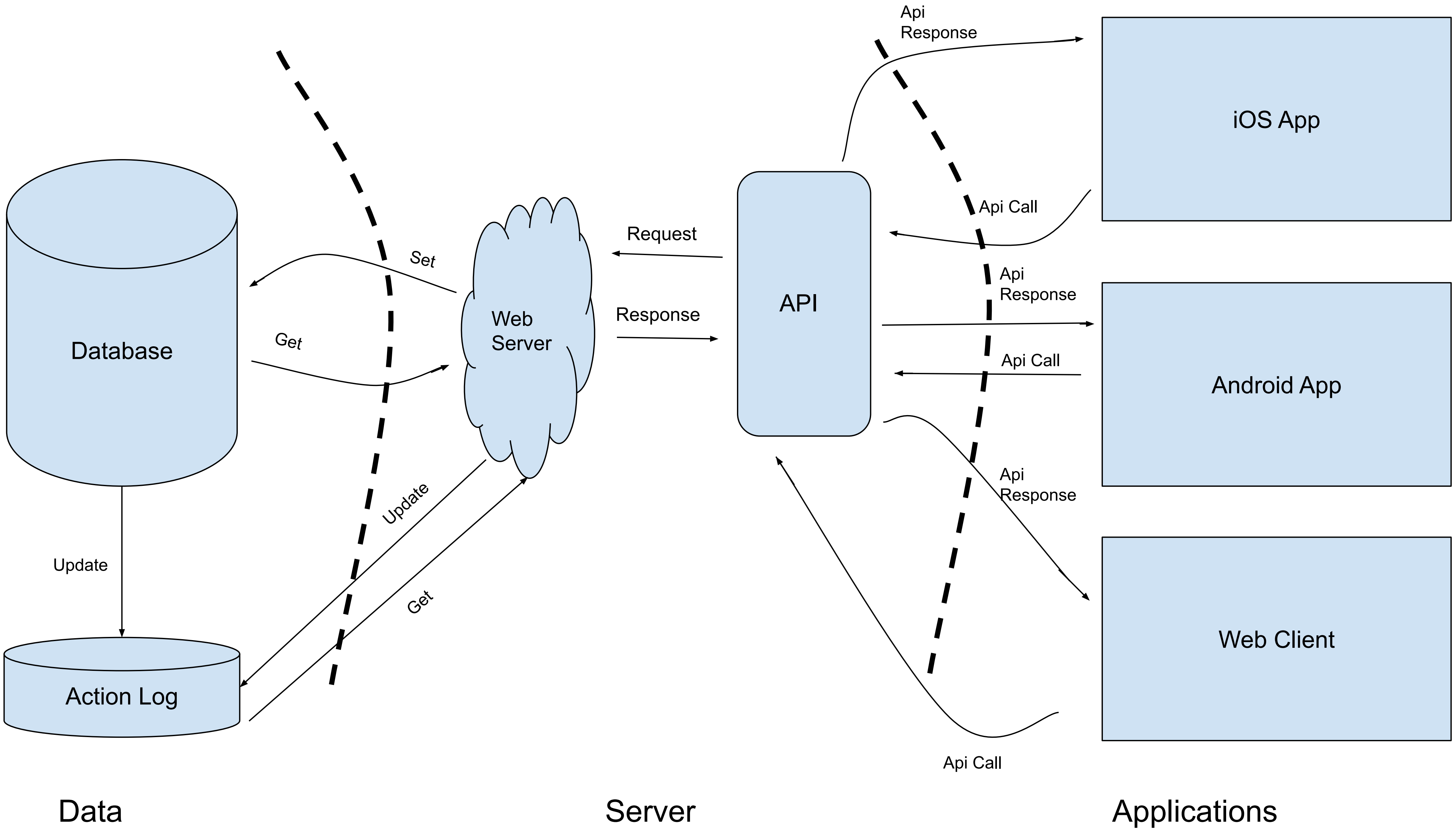
Nick Pandelakis and Owen Barnett
CS 231
3 May 2021

Attacks:

1. People could steal passwords and get someones data
    a. Two factor authentication to protect people's personal information. (S)
2. Someone could make an account and pretend to be someone
    a. Require an email to make an account, this won't stop the issue completely but it will make it harder to pretend to be someone else without burdening the users too much. (S)
3. People could use an SQL injection attack on the database with some of the features
    a. Make sure that we store user input properly and check for escape characters. (T)
4. There could be someone who post multiple false citing to try and discredit the data
    a. We can have a reporting system or moderation system to make sure people are posting accurate information. (T)
5. Someone may do something illegal on the platform
    a. Make sure data is signed so data can be traced if necessary (R)
6. An attacker could want to make changes to the database without leaving a trace.
    a. The application can update a log of changes made to the database (R)
7. A trusted individual may steal credit card information without being caught
    a. Make sure that even for trusted individuals looking at data is logged so they can be caught and punished (R)
8. People could eavesdrop on the API calls and responses and among other things steal usernames and passwords
    a. Encrypt the data using HTTPS/TLS. (I)
9. A trusted individual may try and steal users passwords
    a. Make sure that passwords are not directly stored instead store the hash of the password and salt (a random string). (I)
10. Someone could try and overload the server with too many request (DDOS)
    a. Have a backup server and attempt to identify and remove malicious network traffic. (D)
11. Someone could reset other people's passwords to stop them from logging on
    a. Use the email the user gave when creating the account to reset their passwords. (D)
12. Someone with access to the web server could try to update the database to elevate their privilege and gain direct access to the database.
    a. We could make such an update request possible only indirectly. I.e. in order to gain elevated privilege, someone else with higher privilege must add you to the database, you cannot add yourself. (E)


Api
Response
iOS App
Api Call
Request
Set
Web
Server
Response
API
Api
Response
Database
Get
Api Call
Android App
Api
Response
Update
Update
Get
Web Client
Action Log
Api Call
Data
Server
Applications