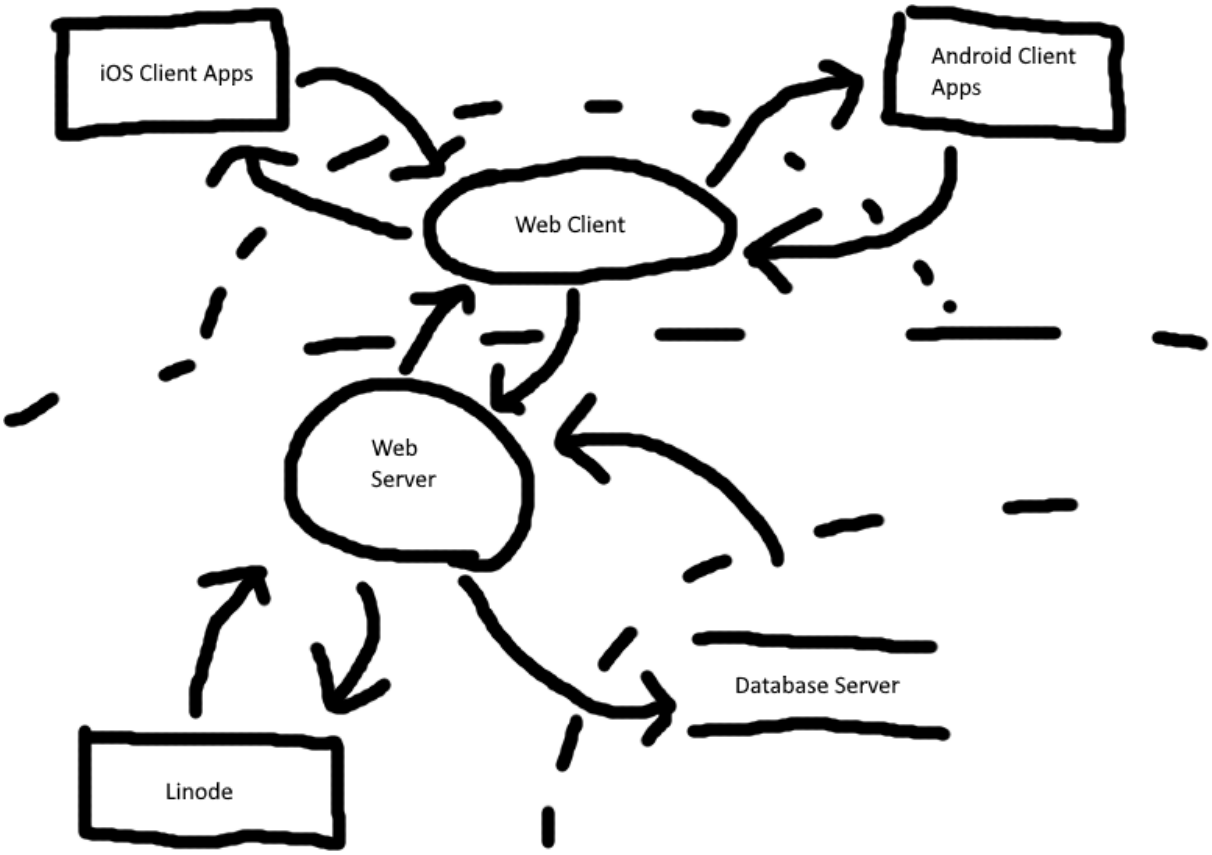
John Woods

Threat Analysis Using Stride

First, the dataflow diagram:



Now, for the STRIDE threats.

Spoofing: This one's pretty obvious. Someone in the apps could spoof themselves as another user, accessing their very important tapir photos or other details. This could be done by watching them enter their password, or via other means of obtaining. There's also the possible threat of someone spoofing as the webserver, via manipulation of certificates or perhaps a secret key leak. Someone could potentially make an account in someone else's name, impersonating them and claiming terrible things (such as preferring pandas to tapirs). Finally, someone could spoof as a plumber or technician in real life and walk into Jeff's home office to interact with the server directly.

Tampering: Once gaining access, someone could modify or edit crucial tapir details, thus messing with the system. Someone could also spam someone's inbox with photos of pandas instead of tapirs, messing with their ability to easily admire said tapirs. Finally, someone could tamper with data by corrupting or destroying it, perhaps by walking into Jeff's office and spilling coffee into his computer.

Repudiation: This one's tough, but if no proof or identifiable info was required to make an account, someone could make a completely anonymous account and post harmful things with no accountability (such as saying that tapirs look silly and that pandas are much cuter). Given that Tapirs Unlimited is a social media, while we could link an account to an action pretty easily, linking that account to a real person might prove much more difficult.

Information disclosure: First, someone could leak the sordid details of their private conversations and DMs with another user, revealing to the world that they're a dirty panda fan. Alternatively, someone could hack into the webserver or just simply steal Jeff's computer, and use that to leak the entire contents of the website, in particular their contact and credit card details.

Denial of Service: This one could be the classic method of just making tons and tons of requests to the server, perhaps through a botnet. However, another method could be something as simple as bashing Jeff's computer with a hammer, or burning down the building holding the Linode server rack. Turning off the power to the webserver, jamming Jeff's wifi to take down the database, or adding a virus to the site that infects client phones and deletes their apps, or deletes their accounts.

Elevation of Privilege: A malicious user could convince the website that they're an administrator, or that they're a Linode developer, allowing them to do things a normal user could never accomplish. They could also pose as a police officer, giving them the supposed privilege to enter Jeff's house and mess with the database.