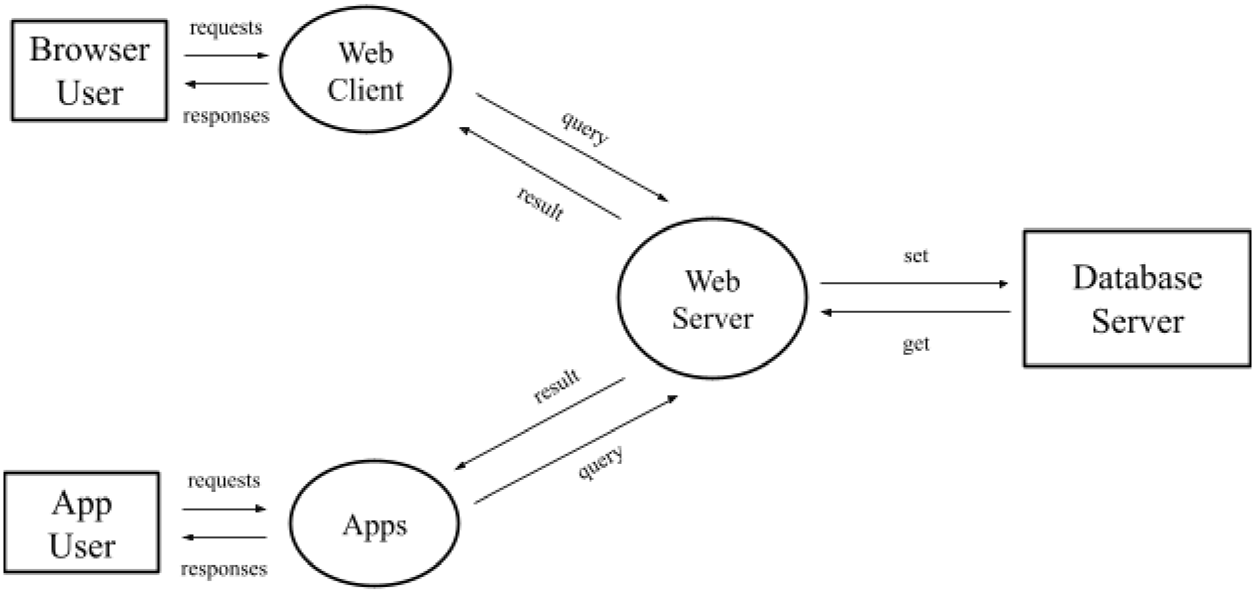
Mary Blanchard and Kaitlyn Peterson



S - Spoofing

Threat: A malicious attacker impersonates the web server. Mal makes a request for information about several users, and gets sent back their addresses, names, and credit card information, which he uses in his other malicious endeavors. (Similar impersonation threats are possible with Mal impersonating any other entities in the data flow diagram).

Mitigation: The web server and database server should use digital certificates and perform the necessary checks (with random numbers encrypted with their secret keys) to determine the entity they are talking to is indeed who they say they are.

Mitigation 2: Another possible mitigation to this threat is to use Linode’s database feature to store information, rather than storing data on Jeff’s computer in his home office. This would reduce necessary communication over open channels.

Threat: A user steals their buddy’s password, and uses it to log in and post inflammatory anti-tapir content.

Mitigation: The website should require two factor authentication. It should also have certain requirements when creating passwords, so users are forced to create a password they have not used before.

T - Tampering

Threat: A malicious attacker Mal intercepts tapir location data being sent from the database server to the web server. Mal receives the correct location data from the database, alters it, then sends it onto the web server. Now, when users want to look at location information about tapirs and search for them in the wild, they find no tapirs in the locations indicated by the website.

Mitigation: All interactions between the web server and the database should be encrypted using TLS over an HTTPS connection.

R - Repudiation

Threat: Attacker pulls sensitive information on tapir locations or deletes all of the images of tapirs from the web server, but claims to not have done that.

Mitigation: The web server keeps a log of all of the requests (read and write) made to the database server. This log is stored separately from the database server so that someone couldn't just go in and edit it. This could be implemented and stored by the web server and/or the host of the web server, Linode.

I - Information Leak

Threat: An eavesdropper listens in over an open network communication between the web server and the database server. The eavesdropper discovers personal information such as credit card numbers and addresses, and even secure tapir locations.

Mitigation: All interactions between the web server and the database should be encrypted using TLS over an HTTPS connection.

Threat: A certain user has a private account on tapirsunlimited.com; the personal pictures and location tags are only available to those who are friends with the user on the site. The attacker wants to know this user's private tapir interactions. They employ a brute force attack by trying a dictionary of common passwords. They successfully log in to the user's account and are able to see all of this user's private information, (and the information of all the user's friends).

Mitigation: After a certain amount of incorrect password attempts, users should be prompted to reset their passwords through an email (to which the attacker would not have access). This would prevent the attacker from being able to perform the brute force attack.

D - Denial of Service

Threat: Attacker writes a script to make many accounts, all of which try to upload videos of tigers, jaguars, poachers, and other threats to tapirs via large files. This data upload and any subsequent vetting of video subjects would put enough strain on the web server that service would become slow and unavailable to many users.

Mitigation: Captchas and other requirements for new accounts should be put into place. These need to be implemented by whoever sets up the web server (Jeff?), but the feature availability falls to the web server host, Linode.

E - Escalation of Privilege

Threat: User is a student or coworker of Jeff and knows a lot about his life. They are able to reset Jeff's admin account password using security questions, since they know the answers. Now they have Jeff's admin access and could do many harmful things.
Mitigation: Password resets should require email verification or some other secondary identity check besides simple security questions. Additionally, Jeff could share less about his personal life with those who may have anti-tapir sentiments.

Another threat to consider, which could involve all of the STRIDE categories:

An attacker breaks into Jeff's house and logs into Jeff's computer hosting the database using Jeff's top-secret password which he has left on a sticky note stuck to the monitor.

Spoofing - the attacker is able to pretend to be Jeff/the admin of the database server.
Tampering - the attacker can directly change information stored on the database server.
Repudiation - the attacker would be able to claim that Jeff was the one who tampered with the server, since they were logged in as him.
Information leak - the attacker gains access to the information stored on the database server, such as the locations of endangered tapirs, or private user data.
Denial of service - once they have finished pulling information, the attacker could take Jeff's computer, effectively ruining all functionality of the website.
Escalation of privilege - again, since Jeff is the one hosting the web server, he has admin access. The attacker is able to gain this admin access when they break into Jeff's house.

Mitigation Tactics:

One great way to mitigate all of these threats is by increasing the security on Jeff's house in order to prevent a break-in. Jeff could also host the database server somewhere other than his personal computer in his home office. Despite wanting all of the fame and glory of founding this incredible website, Jeff could also keep it a secret that he is the one who founded tapirsunlimited.com in order to prevent people from looking up his address and attempting to steal his computer.