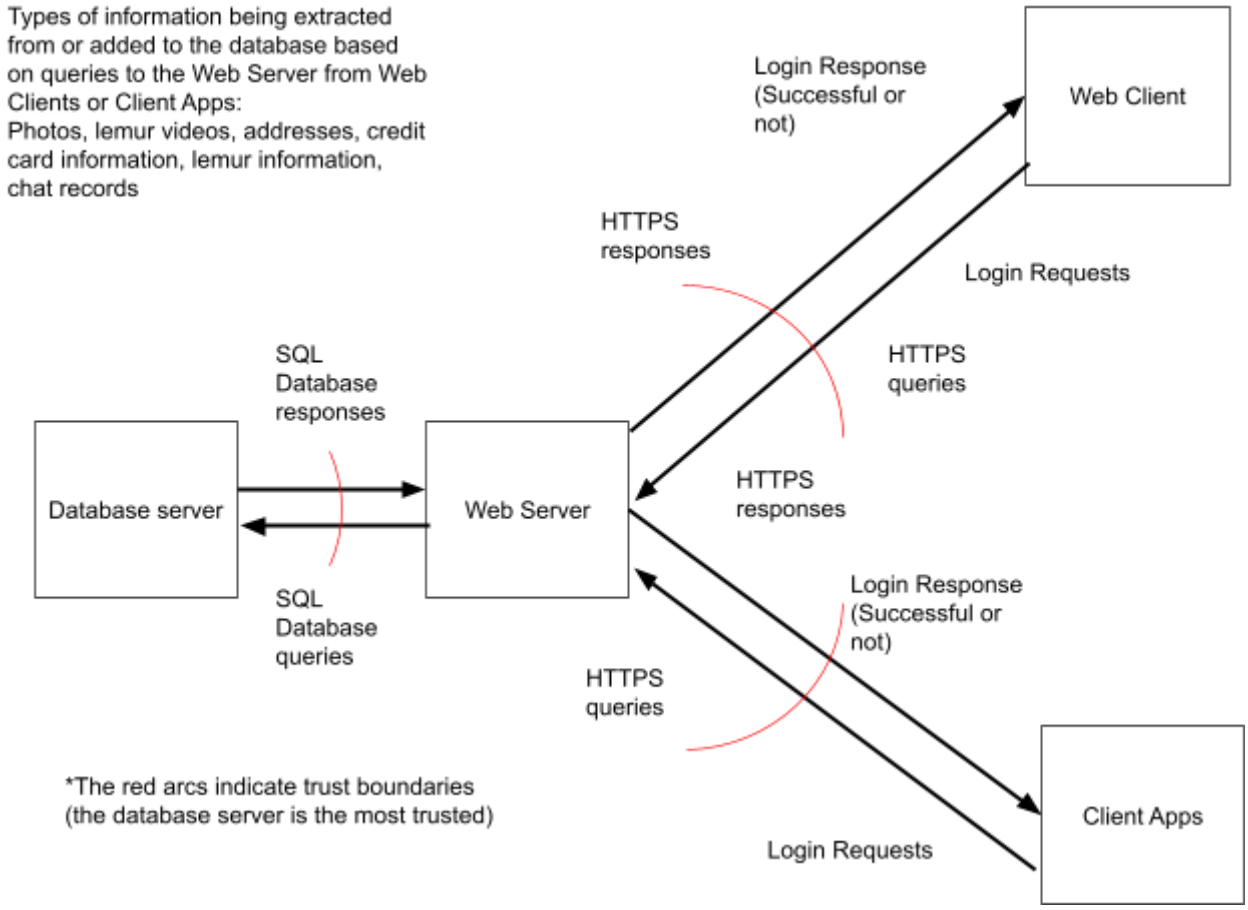
Kevin Clelland and Josiah Misplon

Data flow diagram:



STRIDE Threat Analysis:

Spoofing:
Threats:
-A user directly obtains someone else's login credentials (through phishing or something similar)
-Password attacks on accounts that have weak passwords

Mitigation:
-Require two-factor authentication so that more must be obtained than just login credentials to gain access to an account
-Implement a minimum password length, and check against common passwords

Tampering with data

Threats:
-Some jerk keeps deleting lemur pictures and replacing everything with cat pics (users can alter data)
-Disgruntled lemur hunter walks into DLN's office and replaces all of the lemur photos in the database with pictures of cats through direct physical connection with the database.

Mitigation:
-Only the user who posted information may change it (delete/modify request must contain credentials in a header field)
-Implement basic physical security measures (like locks or hiding the location of the servers) to protect the webserver and database from unauthorized physical access.

Repudiation
Threats:
-People uploading bad data anonymously
Mitigation:
-Require user accounts, and maybe have a minor fee or a wait time to discourage trolling

Information disclosure
Threats:
-Someone is packet sniffing the lemur users
-Remote users are able to get into the server and see user information such as passwords and credit card information

Mitigation:
-Encrypt data going between Web server and Clients using HTTPS and TLS
-User data is only stored after being cryptographically hashed and credentials are validated by comparing hashes

Denial of service
Threats:
-A person is creating so much traffic that no one else can access the database
-Wisconsin steals all our lemurs

Mitigation:
-Users are limited to 1 lemur request per minute / use a distributed model
-We ransom their cheese

Elevation of privilege
Threats:
-Disgruntled former moderator/employee/volunteer for DLN's lemur enterprise uses administrative credentials to steal credit card information

Mitigation:
-Institute policies to revoke administrative privileges / access to servers immediately following their termination