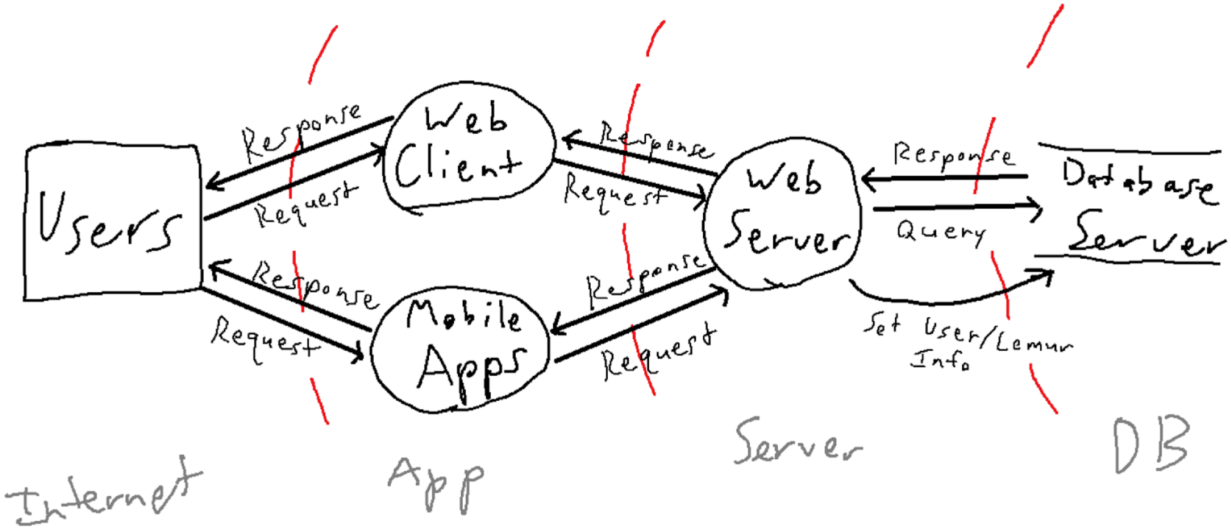
Threat Analysis Using STRIDE

Kenyon Nystrom, Avery Watts, Ben Aoki-Sherwood

Flow chart:



STRIDE threat identification:

- **S**poofing
- **T**ampering
- **R**epudiation
- **I**nformation Disclosure
- **D**enial of Service
- **E**levation of Privilege

Threat	**STRIDE element**	**Mitigation**
Creating fake client to intercept data between user and web server	S	Using https and certificates from a legitimate CA will prevent spoofing between the client and the web server
Unauthorized or malicious actor modifies data in the database	T	Password-protect the database and only give passwords to high-level trusted users. Change passwords periodically so that former employees no longer have database access. Also, use https to ensure only trusted clients can access the database server.

Unauthorized or malicious modification or replacement of web server files.	T	Protect the web server with a password and change frequently. Protect your code base.
An anonymous attacker edits the client or server source code to insert code that sends them all the data that goes through the client and/or server.	R	Only allow source code access to certain individuals/machines/networks (?) with some high degree of authentication. For example, to edit source code, users need to provide their certificates to prove their identities before logging into the editing system, which can then trace their edits to them. This also means that the means of authentication--secret keys, passwords, etc--need to be protected. Also, if editing access is tied to machines or networks, these need to be physically secured.
An attacker uses a botnet to send loads of traffic to our web server, overwhelming the server and bringing it down.	D	Can work to block the attackers' IP addresses. Limit the rate of requests that any given IP can make; use reCAPTCHA to prevent bots from making lots of accounts.
A user convinces the server that they are an admin and gains abilities that they shouldn't have, like taking credit for other users' lemur photos.	E	Make sure all admin actions need strict identification, such as dual authentication. Only registered admin accounts can have admin privileges.
Creating fake web server to intercept data between client and database	S	Use https and make sure the web server uses a password to add, delete, or request data.
Information on the database server is leaked, potentially exposing sensitive information.	I	Store user login info in hashes to prevent access to the actual information. Also significantly limit the database server's ability to interact with outside servers, such that no direct link is made beyond with the web server. Protect the physical location of the server as well.

Somebody ARP spoofs the user’s router and intercepts all the packets sent from their client to the web server.	S/I	All traffic between the user and client is encrypted using HTTPS so even if the spoofer intercepts packets, they can’t decipher them or tamper with them undetected as long as the secret keys of the user and the server remain secret.
A hacker is able to gain access to the system and encrypt all information in the database and on the web server. (Ransomware attack).	D	Password-protect the database and only give passwords to high-level trusted users. Change passwords periodically. Also, use https to ensure only trusted clients can access the database server. Only allow access to the database through the web server. Password-protect your code base for the web server and use https. Make sure all admin actions need a high level of authentication so malicious actors don’t have access. Have backups of all information and web server files in an off-site location.
phishing: phishers target employees to gain access to and tamper with the code, or target users to steal their data.	I/T	Educate users and employees not to click on suspicious links. Ensure that any emails sent from the company follow a specific, recognizable format that distinguishes them from phishing emails. Use dual-authentication or another form of authentication for employee actions to help prevent unauthorized access from a possible phisher.