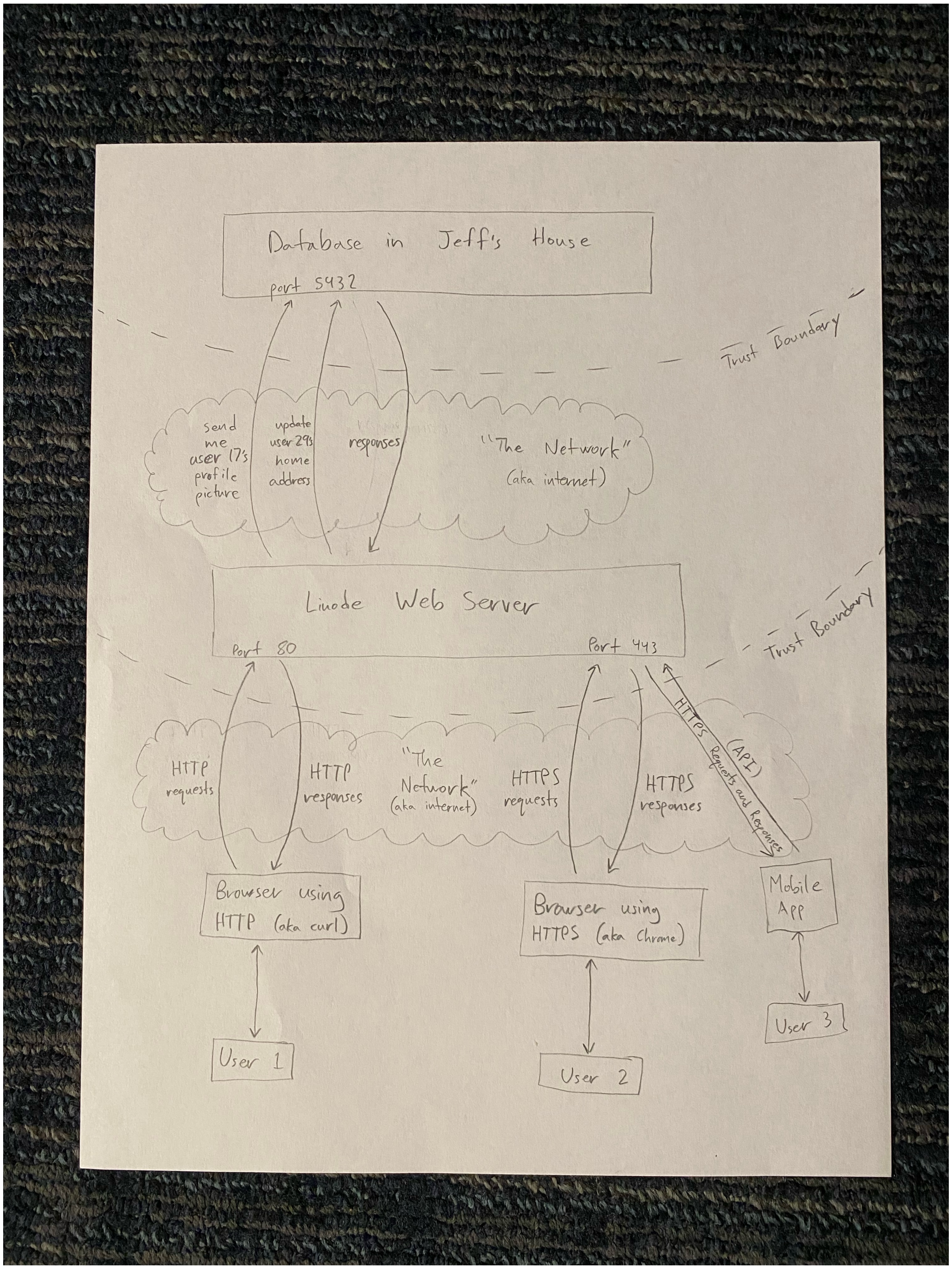
Ben Hafner
Professor Jeff Ondich
CS 338 Computer Security
May 2022
Threat Analysis Using STRIDE

Data flow diagram of hypothetical Tapirs Unlimited social network


Database in Jeff's House
port 5432
Trust Boundary
send me user 17's profile picture
update user 29's home address
responses
"The Network" (aka internet)
Linode Web Server
Port 80
Port 443
Trust Boundary
HTTP requests
HTTP responses
"The Network" (aka internet)
HTTPS requests
HTTPS responses
HTTPS (API) Requests and Responses
Browser using HTTP (aka curl)
Browser using HTTPS (aka Chrome)
Mobile App
User 1
User 2
User 3

Threats and mitigations

Spoofing

Mal could pretend to be the Tapirs Unlimited website so when a user tries to log in, Mal would get their password. This threat can be mitigated if the user uses HTTPS instead of HTTP and checks to make sure the website they're logging into really does have the certificate of Tapirs Unlimited. For the same reason, the app version of Tapirs Unlimited should also communicate over HTTPS instead of HTTP.

Also, a random person could establish a TCP connection to port 5432 of the database and ask for user data, pretending to be the web server. To prevent this, the database should require the web server (or whoever is pretending to be the web sever) to show its certificate and prove that it has the corresponding secret key before sending any data.

Tampering

Someone operating a router in between a user and the web server (or between the web server and the database) could purposefully or accidentally alter the data being sent across the network. In response to this threat, all data should be sent with a checksum, hash value, MAC, or some other data integrity protocol so that the receiver knows if the data has been tampered with.

Repudiation

Mal could make a post that says "I'm Alice and I just killed a Tapir." If people really believed Alice authored that post, they'd all hate her. To prevent this from happening, there should be a secure way that posts are associated with the users who posted them. Then Alice could repudiate Mal's false claim by saying "I didn't write that post at all, it actually says it was posted by your account Mal!" Then everyone would have Mal.

Information Leak

If the communications between the web server and the database weren't encrypted, Eve could listen in and see everyone's data. Obviously, to prevent this, combinations between the web server and database should be encrypted.

If Jeff has admin access to the database, he could potentially look at individual users' data and posts. Jeff could see user's home addresses and stuff on the database, which would be a privacy violation. To mitigate this threat, the database could be encrypted somehow in a way that even Jeff couldn't decrypt.

Here's another one: the NSA could (and probably does) monitor the network traffic to and from the web server. Suppose for example that a group of protesters decide to use the direct messaging feature of Tapirs Unlimited to coordinate a protest against government sponsored Tapir abuse. Even though the communications are encrypted, the NSA could still track down what IP addresses were actively communicating with the Tapirs Unlimited web server during the protest and then use those IP addresses to track down where the protestors live. I can't really think of a practical way to mitigate this threat.

Denial of Services

Mal could use a bunch of proxies to all make knew accounts on Tapirs Unlimited at the same time and then each account could start uploading millions every second. The web server would be overwhelmed and no one would be able to access Tapirs Unlimited until Mal stopped spamming the server. To prevent this, the web server could temporarily block users who request to post at an extremely high frequency (more than once a second or something).

Elevation of Privileges

Suppose Jeff’s daughter happens to know all Jeff’s passwords. Then she could log in to the Tapirs Unlimited database or web server with Jeff’s admin privileges. To make this attack harder, the server and database could require two factor authentication to log in with admin privileges.