Kiefer Lord
CS338
6 May 2022

STRIDE Homework

Spoofing

- Mal could create a fake web client or app posing as the real one
- Mal could create a fake web server to talk to the web client/app
- Mal could create a fake database server to talk to the web server
- These attacks could be mitigated using the public key infrastructure and certificates

Tampering

- Mal could use the above spoofing techniques to manipulate the data being sent through the network
- If HTTPS was being used, we could tell that someone was tampering because we would see gibberish being sent around the network

Repudiation

- Mal could tamper with the database server to remove his search history (for example), allowing him to repudiate any claims about his search history
- HTTPS would prevent tampering

Information Leak

- Mal could leak users' credentials and activity if he had sufficient privileges on the database server
- The is mitigated by the fact that only the system administrator has those privileges, but this person would be able to leak the user information

Denial of Service

- Mal could create a bunch of accounts and flood the network with traffic. This could be prevented by not allowing one person/email address to create more than one or two accounts.
- Mal could sever any of the connections in the data flow diagram, maybe by unplugging one of the servers. This could be prevented by keeping the servers physically secure.

Escalation of privilege

- Mal could give himself sudo privileges on any one of the servers involved. I'm not sure about exactly how this could happen, but Mal could potentially break into your office and create a new user with sudo privileges on the machine. This could be prevented by keeping the servers physically secure.

Data Flow Diagram