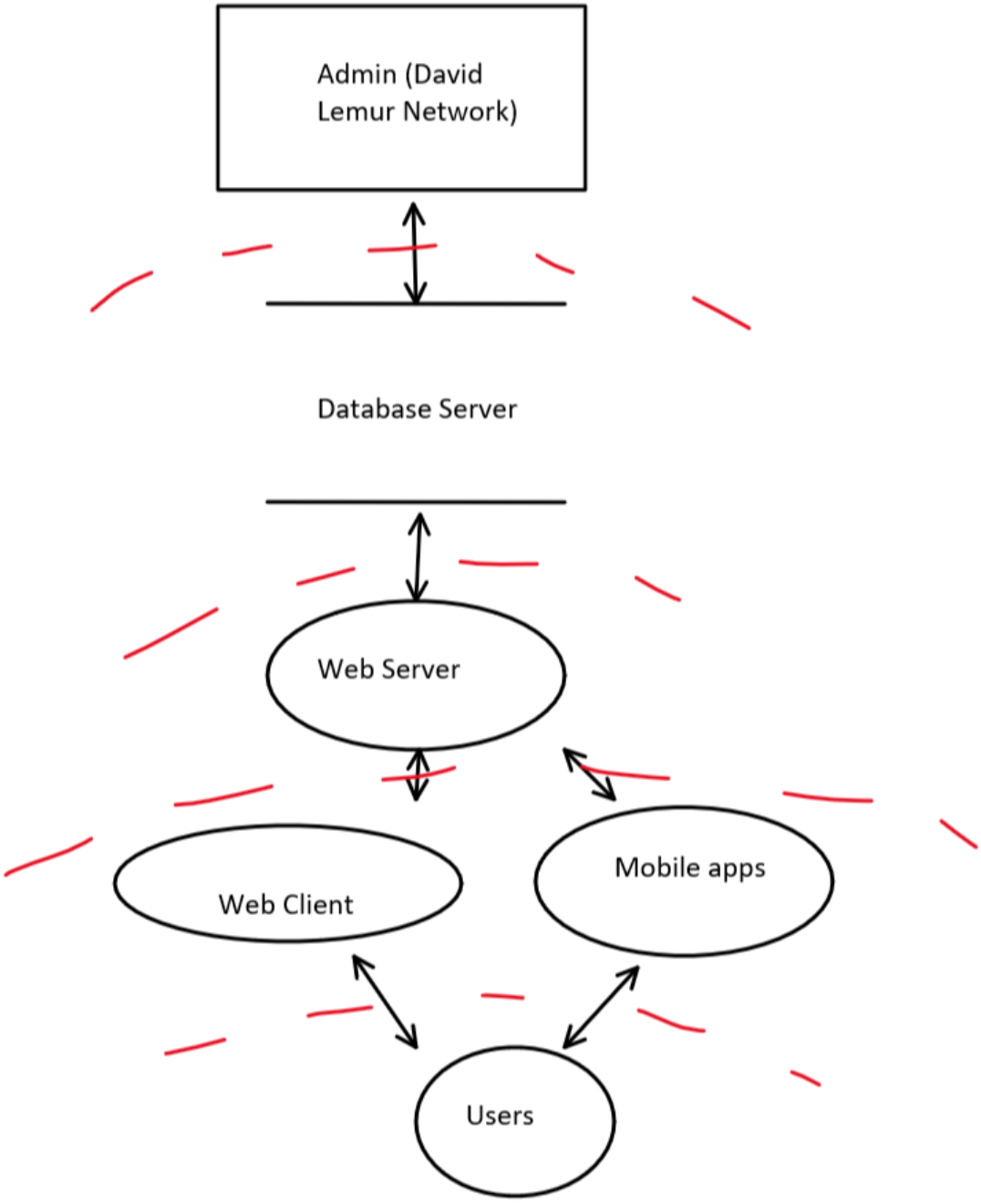
Eric Gassel

STRIDE Analysis of the David Lemur Network



Spoofing

Threat: Someone could impersonate another user on the web server in order to gain access to information on the David Lemur Network they otherwise would not have access to (such as credit card & other personal info).

Mitigation: Dual authentication, HTTPS

Threat: Fake client apps could trick the system into thinking they have a secure connection but instead are malicious. They would then be able to steal personal data or potentially plant malware.

Mitigation: Verify certificates from potential web clients in order to establish a secure connection

Tampering with data

Threat: SQL injection would allow a malicious user to tamper with & extract info from the database.

Mitigation: Parameterized statements

Threat: A malicious person who could impersonate admin (if they stole passwords) in order to gain access to the database server and tamper with data.

Mitigation: Dual authentication, admin authentication

Repudiation

Threat: A malicious person could delete or modify usage/access control logs in the database, making it difficult or impossible to track the actions of any given user.

Mitigation: Encrypt database information, hash database information to maintain integrity

Information disclosure

Threat: A malicious person could eavesdrop on the interactions between database and webserver

Mitigation: use HTTPS which encrypts the messages passed between the two

Denial of service

Threat: A malicious person could gain access to the web client and deny information from the web server for the user.

Mitigation: HTTPS would provide a greater barrier to gaining access to web client, require certificate verification

Elevation of privilege

Threat: A malicious person could elevate their security clearance to admin in order to access database information they should not have.

Mitigation: Admin authentication, access control logs