Jack Huffman collaborated with Doug Pham
CS338 Computer Security
Jeff Ondich

Spoofing - There are many possible ways that one may use spoofing to infiltrate Tapirs Unlimited, one method would be through the use of phishing emails with a fake login page. If a legitimate user of Tapirs Unlimited received a seemingly legitimate email from someone posing as Tapirs Unlimited they may be inclined to follow their link to a fake login page to Tapirs Unlimited. If this happens they would likely input their username and password combo with which the adversary could use to access their account on the real Tapirs Unlimited network. To prevent this users should look carefully at the email addresses of senders and look for red flags. Additionally, whenever they are following links they should first look at the URL and ensure that it points to the proper destination rather than something that might look right but has a couple characters off.

Tampering - An adversary of Tapirs Unlimited could possibly exploit tampering if they were able to acquire administrators credentials. If they achieved such credentials, they would have authorization to alter the database of Tapirs Unlimited to whatever they wish (maybe something as evil as Anteaters). To prevent this, those with administrator access should be extremely careful with their login details and not fall victim to phishing or poor storage of their password.

Repudiation - An example of a repudiation threat with Tapirs Unlimited could be that a user makes a harmful post by posting an Anteater or some other animal (which is strictly prohibited) and claiming that they did not make such a post. To prevent this from happening Tapirs Unlimited should ensure that they do not allow unregistered individuals to make posts on their site. Additionally, with all users logged in the site should also keep track of which user made which post to the site to ensure that all posts can be traced back to a user.

Information Disclosure - A potential insecurity with Tapirs Unlimited could be if they use only Basic Authentication to transmit login information between the client and server. If there was a lack of this security then it is possible for an eavesdropper to be able to spy on the transmission of data and retrieve sensitive information. This would obviously create an insecurity in the system which could lead to the integrity of Tapirs Unlimited to be compromised. To prevent this from happening, Tapirs Unlimited should secure their communications with TLS and use HTTPS as opposed to HTTP.

Denial of Service - A potential adversary of Tapirs Unlimited (an upstart competitor Anteaters Unlimited) may wish to deny users access to the web server, they could do this through a DDoS attack (Distributed Denial of Service Attack). This means the adversary would flood the open ports of Tapirs Unlimited with malicious requests to stall real users' ability to access the web

server. One way that Tapirs Unlimited could prepare for this would be to increase the bandwidth that the server is operating on. This would make it so that the potential attacker would need to allocate significantly more resources in order to affect the performance of Tapirs Unlimited. While this doesn't prevent a DDoS attack from happening it will help protect users access to the server if Tapirs Unlimited does come under attack

Elevation of Privilege - A potential threat for Elevation of Privilege would be if someone using the Client App on IOS or Android found a vulnerability in the IOS or Android system which allowed them to elevate their status to administrator status. This would allow them to have authorization to sensitive information on Tapirs Unlimited which they would not normally have access to. To prevent this, mobile users should make sure that they keep their IOS and mobile app updated as frequently as possible. Additionally, the Tapirs Unlimited app should use proper verification and ensure the users are not able to alter their own access rights. Much of this insecurity may lay on the hands of the IOS and Android developers to ensure there are no faults in their software but the Tapirs Unlimited mobile app developers should also ensure that they take these precautions to ensure proper authorization.