Jonathan Disla

Assignment 9.1

Web 420

Prof. Krasso

Within the process of securing an application we have to authenticate users in order to authorize them access to data. According to Okta, “authentication is the act of validating that users are whom they claim to be.” Furthermore, authentication establishes ownership of a set of data for the specified user to manage. Examples of authentication can be the verification of a users information; entering correct login username and password. With the clause that entering incorrect data results in not being able to proof the information entered is valid thus restricting access. Authorization determines the level of information the user is privy to. For example, an admin user will have access to all the data where a sub user is only granted access to his or her own data only. According to Okta, “In secure environments, authorization must always follow authentication.”

Levels of authentication include: Passwords, one-time pins and biometrics. I spoke earlier about passwords but lately companies are using pins to authenticate users. Pins are temporary or usable only for that session. Biometrics are more often used on cell phones in the form of fingerprints or eye scans. There are also mixed forms of authentication which is called two step authentication.

The first status code I selected is 408 or request timeout. The response is sent on an idle connection by some servers...it means that the server would like to shut down the unused connection (Mozilla). Another HTTP status code is 503 or services unavailable. This code appears when a server is not yet prepared to receive a request. According to Mozilla MDN, a common cause for this code is when a site is down for maintenance.