Dumbstruck Gold

Security Threats assessment

Security Threat 1: Code Security

When creating enterprise software you often have competitors doing something similar and if your company is succeeding people will try to emulate you or steal your secrets to success. For software the secret to success is the code itself. In order to stop malicious parties from stealing our code we could use code obfuscation. Code obfuscation is the practice of making something difficult to understand. Code obfuscation is used to protect intellectual property as well as to prevent attackers from reverse engineering proprietary software. Obfuscation can involve things from encrypting some or all of the code, stripping out potentially revealing data, renaming variables to meaningless names, among other things. A site that preforms this on JavaScript code for free is available here: https://obfuscator.io/

Security Threat 2: Unauthorized use of code

Securing accounts especially for paying customers is a big deal in computer security and always will be. To make sure that the accounts of paying customers are secure the website that hosts our software will have to have minimum password requirements such as an 8 character count with a special character and a number included. These passwords when stored should also be encrypted in case someone unauthorized gains access to the databases. This way they will not be able to steal the passwords which may be reused on another site by the same user.

Security Threat 3: Unsecure Camera feeds

Another threat to security is malware that can spy on you. When using a camera with malware or viruses on a computer without antivirus software, users open themselves up to the threat of being spied on. To combat this before starting our software we should display a popup warning users of this threat and try to implement a way to check if they have antivirus installed before starting up the camera feeds. This will help protect them and remind them to make sure their computers are secure.