Hector Gomez

3/4/2024

CYSE 368

Reflection Paper 4:

We completed 200 hours of the internship and turned in the technical blueprint and a PowerPoint presentation. Within the presentation, we added information regarding the system security for the VR headset. User Authentication: VR headsets may employ various methods for user authentication, such as passwords, PINs, biometric authentication (e.g., fingerprint or facial recognition), or even more advanced methods like iris scanning. This ensures that only authorized users can access the device and its content. Data Encryption: Encryption is essential for protecting sensitive user data stored on the VR headset or transmitted between the headset and connected devices. Encryption algorithms such as AES (Advcanced Encryption Standard) may be used to secure data, including user profiles, payment information, and communication with external servers. Secure Boot: Secure boots ensures that only trusted software components are loaded during the boot process, thereby preventing unauthorized or malicious software from running on the device. This helps protect the integrity of the VR headset's operating system and fireware. These were a few things we added within the powerpoint to send up to the big boss persay for approval. We had a ton of meetings after we finished the powerpoint to add finishing touches and talk about whats next. The next following 50 hours of this internship we will be developing the grounds of 3 firewalls for the VR headset. This completes the 200 hour mark of the internship and I am excited for what is to come. Down below are some links that we used for the powerpoint. Thank you.

https://ieeexplore.ieee.org/document/10179367

https://cribbcs.net/vr-headsets-what-you-need-to-know/#:~:text=Data%20is%20encrypted%20at%20rest,1.2%20and%20TLS%201.3%20protocols.

https://semiengineering.com/design-and-security-challenges-for-vr/#:~:text=For%20example%2C%20secure%20boot%20verifies,these%20devices%20become%20more%20mobile.