**Suggestion from Dr. Jacobson:**

* “Using encryption between the server and the headset. You could do something as simple as TLS, which there are open source libraries for. That way you could also authenticate the server and even the headset using the hardware addresses or some other ID. SSH is another protocol that could be used, again open source libraries. The choice will depend on the other libraries you are using and the O.S. as to which is easier to integrate. TLS is more of an O.S. layer and SSH is more application layer.”

**Links/Notes from Dr. Rover:**

<https://twitter.com/science_punx/status/1304443456262111235>

<https://www.theguardian.com/australia-news/2020/jul/01/ceo-of-exam-monitoring-software-proctorio-apologises-for-posting-students-chat-logs-on-reddit>

* Students chatlog publicly posted by Proctorio CEO
* Who should have access to the data gathered, how long should that data exist, can AI be used instead

<https://www.insidehighered.com/blogs/just-visiting/choose-cooperation-and-collaboration-rather-surveillance>

<https://www.insidehighered.com/blogs/university-venus/unfeeling-ai-and-assessment>

<https://www.insidehighered.com/digital-learning/article/2017/05/10/online-exam-proctoring-catches-cheaters-raises-concerns>

<https://www.insidehighered.com/blogs/university-venus/response-proctorio>

* Look into issues faced by Proctorio and how they apply to our project
* Consider having a security team

**Existing Proctor Companies**

* Proctorio: monitors student during exam with video/audio/key strokes, flags suspicious things and all is sent to professor
  + Con: up to the proctor/teacher to review it all

**Security for products on market**

* Oculus for Business:
  + Multiple layers of encryption
  + Machine learning
  + Log into app that connects to headset by bluetooth
  + <https://business.oculus.com/security/?locale=en_US>
* Google Glass
  + Security concerns:
    - recording when people don’t know, supposedly a light goes on when recording but this could somehow be disabled by future apps
    - Could be hacked and hacker would have access to everything someone sees

**Security Techniques**

* Breaking up into bits and sending pieces in different ways
* Encryption
* VPN
* SSL, FTPS, SSH

**Ensure Identity**

* biometric authentication through eye scan

**Other topics to look into**

* White and black lists in lock down browser