Milestone 2 Report
CSCI 4800

Group Members:
Jay Washington
Landon Murdock
Ja'Von Holmes
Solen Makonnen
Richard Mauzy

Sources:
Links to harms related to zoom bombings:
https://www.nytimes.com/2020/04/03/technology/zoom-harassment-abuse-racism-fbi-warning.html
Paper about a zoom bomb:
https://seclab.bu.edu/people/gianluca/papers/zoombombing-oakland2021.pdfhttps://seclab.bu.edu/people/gianluca/papers/zoombombing-oakland2021.pdf

Group website: https://nmauzy2.github.io/HCI_term_project/

Group repository: https://github.com/nmauzy2/HCI_term_project/tree/gh-pages

Students conspire in chats to Zoom Bomb:
https://www.pcmag.com/news/students-conspire-in-chats-to-zoom-bomb-online-classes-harass-teachers

Links to existing solutions for zoom bombing:
https://www.pcmag.com/how-to/how-to-prevent-zoom-bombing
Objective Answers:

A. Zoom bombing is the act of disrupting a zoom call, the intention is to disrupt the class. People who Zoom bomb do so by sharing their screen with something obscene such as a pornographic image, or a racist image (For example, showing a picture of a hanged black man out of context during a zoom call about celebrating Black History Month). It's relevant in the context of hybrid synchronous classes because zoom bombing disrupts the zoom call and disrupts the class in progress.

Goal: Disrupt the hybrid/online class.
Plan: Decide which class you are going to bomb
Specify: Attend the class at a particular time and have your obscene imagery/video or mic ready
Perform: Attend the class for a few minutes and then screen share your obscene image/video,

Perceive: Check the reaction of the class or teacher
Interpret: Did they react to what you did?
Compare: If the teacher/class reacted to what you did and are if they are taking the time out to deal with you then you've disrupted the class.

This can be considered a typical way of disrupting an online or hybrid class because some students can organize doing this with others on applications such as Discord, Groupme, etc.

The users in relation to Zoom Bombing for classes would be the professors/teachers since they are the ones who are setting up the zoom meetings and also teaching the class. Additionally, there would be students who have to login and navigate the additional security settings.

B. Analysis of existing solutions

1. Zoom offers some built in ways to help stop zoom bombing. These include creating waiting rooms, blocking guests from sharing screens, locking meetings after they have started, and kicking users from the zoom call. Waiting rooms allow the host of a meeting to control who can enter the call, but the downside to this is that the host has to manually let individual users in and this can be tedious, especially for larger meetings. Blocking guests from sharing screens is a good option to limit the ways that zoom bombers can show disruptive images, but it also places limitations on other users that may not always be ideal. Locking meetings after they start does not stop zoom bombers that join before the meeting is locked, it would also stop students they may join late, or may need to leave and rejoin the meeting. Finally kicking users from a zoom call is reactive, so the zoom bomber may not be removed from the meeting until after they have already completed their disruptive activity.
2. The existing solutions focus on 3 main things. The first is stopping zoom bombers from making it into the meeting in the first place. The second is limiting the abilities of users once they are in a zoom meeting to stop them from being able to perform disruptive actions. The third is removing users from the zoom call if they are being disruptive.

C. Proposed Solution:
Creation of random zoom links + waiting room (currently)
Using your student ID, password for your student ID, and then being allowed access into the zoom meeting through a waiting room.

For our solution we would like to create an application that would combine several methods to stop uninvited users from joining online meetings. The proposed tools that we would use to do this include having students login with personal accounts, using unique links for each meeting, and having waiting rooms before users are allowed to join the meetings.

Our solution is more of an add-on to the current solutions. Right now, they are effective, but there's a possibility that a student could share the link to the online meeting and allow people to zoom bomb the class, so trying to prevent them from being able to enter the room entirely is one solution we thought of.