The Security of Remote Proctoring Software

Sarah Nathanson

Abstract

The coronavirus pandemic has made it necessary to switch to remote learning at universities across the world. This has led to an exponential increase in the use of "remote proctoring" applications. Remote proctoring softwares aim to create secure testing environments for students who are taking exams at home on personal devices. These services perform two main functions to detect and prevent cheating. First, they 'lock down' students' devices, preventing them from accessing outside resources during the exam. Second, some programs record students in their homes and use computer vision to flag suspicious behavior. Despite the claims of manufacturers, there has been a little outside research on the effectiveness of these programs.

In this paper, I present my findings on the security and effectiveness of remote proctoring systems. First, I performed penetration testing on two remote proctoring programs. Next, I created proof-of-concept videos to demonstrate cheating strategies that would hypothetically succeed against remote proctoring programs which record students during exams. Finally, I conducted social media research in order to analyze students' perceptions of these softwares.

Acknowledgments

I developed this project for the Brown University course CS2951-E, Topics in Computer System Security. I am thankful to Professor Roberto Tamassia for his support in guiding the direction and development of my research. I am also appreciative of the logistical support that he provided in setting up institutional access to Top Hat Test. I would also like to credit the suggestions and feedback which I received from other CS2951-E students. While developing exploits, I consulted technical resources such as official documentation and developer forums. Lastly, I would like to credit the many anonymous social media users who exposed cheating strategies publicly.