3-20-2024

Do online test proctoring services abide by standard data protections?

Tristan Stapert
Andrew Kramer

Follow this and additional works at: https://scholar.dsu.edu/research-symposium
Do online test proctoring services abide by standard data protections?

Abstract

In the aftermath of the COVID-19 pandemic, schools adopted new software to allow for online learning. Online exam proctoring has seen rapid growth in both K-12 and higher education. The security of these suites is critical due to their extensive access. Online proctoring suites have the capabilities to assess and configure student devices, access the microphone and camera, and view student information in the scope of the exam. This case study investigates the security of data sent over the network using dynamic software analysis and network monitoring while using the Respondus Lockdown Browser.

Background

The surge in online learning post-COVID led to widespread adoption of online proctoring suites, with Respondus' Lockdown Browser serving over 2000 institutions and 200 million exams annually. The significant access these suites have to student devices and sensitive data raises concerns about test integrity and data security. Unlike standard eLearning software, proctoring suites can access microphones, cameras, and configure devices. Security studies on similar solutions reveal vulnerabilities, emphasizing the need to assess if online proctoring solutions adhere to standard data protections during data collection.

Literature Review


Methodology

This research is a controlled evaluation of the Respondus Lockdown Browser using techniques of dynamic software analysis. Tools like Procmom and Wireshark will monitor the software’s interactions and data flow. The evaluation aims to assess the browser’s security regarding user data handling, including attempts to expose data via connection downgrades or fraudulent certificates. Any vulnerabilities discovered would indicate deficiencies in the browser’s data protection measures outlined in the Terms of Service. Reverse engineering or source code acquisition isn’t part of the evaluation due to contractual limitations with Dakota State University and Respondus.

Results and Discussion

Current findings show that under normal conditions, Respondus Lockdown browser does adhere to standard data encryption when establishing and maintaining exam sessions. It has also proven more difficult to force the Lockdown browser to downgrade its security to a weaker or decrypted transmissions. Further research is still required to determine the effects of certificate manipulation. While current downgrade attempts include blocking HTTPS traffic and dropping TLS handshakes, certificate manipulation may prove to be more successful. Concerns with faulty certificates would be prevented if Respondus accurately validates certificates before establishing connections or uses certificate pinning to protect known good certificates in use.

Conclusions

My examination has currently proven that Respondus Lockdown browser protects student data with standard practice network encryption. This ensures that both student data and device data collected and transmitted during an examine is protected from some forms of man-in-the-middle attacks. Furthermore, this network security ensures that exam data remains while in transmission from a student’s device server.

Future research may include identifying the amount of data collected by exam software有信心 of individuals, are virtualized hardware components detected during an examine, can strategic network manipulation lead to successful exams with failed footage.