Dakota State University
Beadle Scholar

Annual Research Symposium | University Publications

3-20-2024

Do online test proctoring services abide by standard data protections?

Tristan Stapert
Dakota State University

Andrew Kramer
Dakota State University

Follow this and additional works at: https://scholar.dsu.edu/research-symposium

Recommended Citation

Stapert, Tristan and Kramer, Andrew, "Do online test proctoring services abide by standard data protections?" (2024). *Annual Research Symposium*. 29.
https://scholar.dsu.edu/research-symposium/29

This Book is brought to you for free and open access by the University Publications at Beadle Scholar. It has been accepted for inclusion in Annual Research Symposium by an authorized administrator of Beadle Scholar. For more information, please contact repository@dsu.edu.

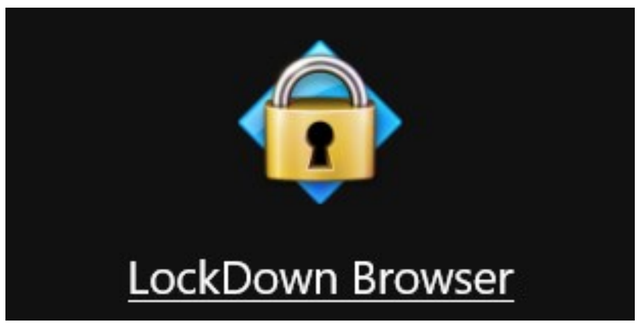
Do online test proctoring services abide by standard data protections?

TRISTAN STAPERT | ANDREW KRAMER

DSU Student Research Symposium **March 20th, 2024**

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.



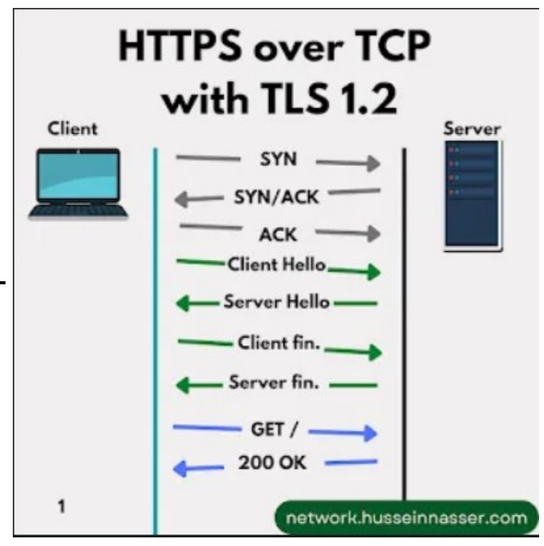
Background

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.

Methodology

This research is a controlled evaluation of the Respondus Lockdown Browser using techniques of dynamic software analysis. Tools like Procmon 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.

Literature Review

[1] A. Terpstra, A. De Rooij, A. Schouten, "Online Proctoring: Privacy Invasion or Study Alleviation?," in *Proceedings of the 2023 CHI Conference on Human Factors in Computing Systems*, Hamburg, Germany, April 2023, DOI:10.1145/3544548.3581181

[2] B. Burgess, A. Ginsberg, E. Felton, S. Cohney, "Watching the watchers: bias and vulnerability in remote proctoring software," in *Proceedings of the 31st USENIX Security Symposium*, Boston, MA, USA, 2022, PDF, Available: https://www.usenix.org/system/files/sec22-burgess.pdf

[3] A. S. Al-Sherideh, K. Maabreh, M. Maabreh, M. Al Mousa, M. Asassfeh, "Assessing the impact and effectiveness of cybersecurity measures in e-learning on students and educators: A case study," *International Journal of Advanced Computer Science and Applications*, vol. 14, no. 5, 2023, DOI: [10.14569/IJACSA.2023.0140516](https://doi.org/10.14569/IJACSA.2023.0140516).

[4] F. I. Khan, Y. Javed, M. Alenezi, "Security assessment of four open source software systems," in *Indonesian Journal of Electrical Engineering and Computer Science*, vol. 16, no. 2, November 2019, pp. 860-881, ISSN: 2502-4752, DOI: [10.11591/ijeecs.v16.i2.pp860-881](https://doi.org/10.11591/ijeecs.v16.i2.pp860-881).

[5] E. Papadogiannaki, S. Ioannidis, "A Survey on Encrypted Network Traffic Analysis Applications, Techniques, and Countermeasures," *ACM Comput. Surv.*, vol. 54, no. 6, Article 123, July 2022, 35 pages, [DOI: 10.1145/3457904](https://doi.org/10.1145/3457904).

[6] R.S. Leon, M. Kiperberg, A. L. Zabag, et al., "Hypervisor-assisted dynamic malware analysis," *Cybersecur*, vol. 4, no. 19, 2021, [DOI: 10.1186/s42400-021-00083-9](https://doi.org/10.1186/s42400-021-00083-9).

[7] C. E. Silva and J. C. Campos, "Combining static and dynamic analysis for the reverse engineering of web applications," in *Proceedings of the 5th ACM SIGCHI symposium on Engineering interactive computing systems (EICS '13)*, New York, NY, USA, 2013, pp. 107-112, [DOI: 10.1145/2494603.2480324](https://doi.org/10.1145/2494603.2480324).

[8] L. Bergmans, N. Bouali, M. Luttikhuis, A. Rensink, "On the Efficacy of Online Proctoring using Proctorio," in *Proceedings of the 13th International Conference on Computer Supported Education, CSEDU 2021*, 2021, [PDF](https://ris.utwente.nl/ws/portalfiles/portal/275927505/3e2a9e5b2fad237a3d35f36fa2c5f44552f2.pdf).

[9] S. Sen, S. Guha, A. Datta, S. K. Rajamani, J. Tsai, J. M. Wing, "Bootstrapping Privacy Compliance in Big Data Systems," in *2014 IEEE Symposium on Security and Privacy*, Berkeley, CA, USA, 2014, pp. 327-342, [DOI: 10.1109/SP.2014.28](https://doi.org/10.1109/SP.2014.28).

[10] Y. Ling, K. Wang, G. Bai, H. Wang, J. S. Dong, "Are they Toeing the Line? Diagnosing Privacy Compliance Violations among Browser Extensions," in *Proceedings of the 37th IEEE/ACM International Conference on Automated Software Engineering (ASE '22)*, New York, NY, USA, 2023, Article 10, pp. 1-12, [DOI: 10.1145/3551349.3560436](https://doi.org/10.1145/3551349.3560436).

Image credits:
https://wireshark.org,
https://medium.com/@hnasr/the-many-configurations-of-https-4fa005a456ad

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 integrity remains while in transmission from a student’s device to their exam server.
Future research may include identifying the amount of data collected by exam softwares themselves on individuals, are virtualized hardware components detected during an exam, can strategic network manipulation lead to successful exams with failed footage.