

Automated Proctoring Solutions: Modern Techniques to Evade & Lure Computerized Proctoring Systems

Roberto D. Solis, Sam Houston State University, United States
Narasimha Shashidhar, Sam Houston State University, United States
Cihan Varol, Sam Houston State University, United States

The IAFOR International Conference on Education in Hawaii 2023
Official Conference Proceedings

Abstract

Automated proctoring solutions are popular tools across multiple types of instruction, including online, hybrid, and face-to-face. Choosing the correct application to proctor online assessments is a tedious process that involves discussions about securing the integrity of examinations and who should absorb the cost of the chosen proctoring solution. Modern automated proctoring solutions are customizable; in most cases, the student absorbs the total cost. Diverse vendors promote using artificial intelligence to detect movement, excessive noise, other persons in the room, or instances of impersonation. We present different scenarios to elude the built-in security features of the Respondus Lockdown Browser and compromise the integrity of online assessments. Windows Remote Assistance, Executable File Analysis, Screen Capture, and Virtual Webcams are practical methods to evade & lure the proctoring application's lockdown capabilities. Moreover, while each procedure may not apply in every scenario, Windows Remote Assistance facilitates the process of impersonation. The application is part of Windows 10 distributions, has no limitations, and setting up a screen-sharing session takes no time and effort. Furthermore, it is possible to leak the content of an online assessment using specific screen capture software.

Keywords: Lockdown Browser, Online Proctoring, Assessment Integrity, Online Learning

iafor

The International Academic Forum
www.iafor.org

Introduction

Online proctoring solutions are a valuable resource for face-to-face and online instructors. Different vendors claim the innovative use of algorithms, but there is no evidence to prove the effectiveness of their software. Increasing enrollment in distance education courses demands alternate solutions to proctoring. Allocating resources for testing is not within the possibilities of institutions that depend on state funds and run under limited budgets. Therefore, instructional departments evaluate solutions with pricing and security being among the deciding factors before implementing a specific proctoring system across the institutions.

Previous work targets academic dishonesty in the form of plagiarism, downloading papers from the internet, paying a third-party platform to write documents, and online sales of test banks and solutions manuals. However, it is essential to consider that all technology, such as web pages, mobile applications, and online banking, may have flaws and limitations within the code. Furthermore, we often read about how big corporations are easy targets for data breaches and attacks from hacktivist groups. Nonetheless, online proctoring solutions are not exempt from flaws or bugs within the code. Many of the proctoring applications are executable files or browser plug-ins, which opens the room for vulnerabilities.

To evaluate the effectiveness of the security measures in Respondus, we demonstrate proof of how to nullify the embedded security mechanisms of the Respondus Lockdown Browser. An online student intending to cheat will attempt to receive help from an external entity. The first successful simulation shows the effectiveness of Windows Remote Assistance. Moreover, Respondus blocks secondary displays, but we exhibit how to enable a second monitor and use lecture notes during an examination. Then, we transition into screen recording, a valuable method to leak the content of online examinations to the entire class. Finally, we mount a virtual webcam and pre-record the verification process. All four methods work with no warnings.

The rest of the paper is structured as follows: background and related studies in section II, definitions and tools in section III, methodology in part IV, simulation results in part V, and conclusion with ideas for future work in part VI.

Literature Review

Cai & King (2020) discuss how the application of instructional technology aids in delivering instruction, such as online assessments during times of crisis. The proposed framework for evaluating proctoring services covers three different types of proctoring services. First, they provide an overview of automated proctoring solutions, which use a combination of features such as machine learning and artificial intelligence to validate the authentication of the exam. Second, we see an overview of the technology behind browser lockdown applications, limiting the number of devices a student can use during a given assessment. As a third option, live proctoring solutions are also available, and they rely on the human factor to authenticate the session before an exam takes place. Even though we have several features to consider in proctoring systems, factors such as cost, training, and support are among the factors that can aid in deciding on adopting a proctoring solution. The main recommendation is to use a combination that implements several features to validate the integrity of the exam.

In research from Lubarda et al . (2021), Oral examinations demonstrate success for high enrollment courses within the engineering and mechanical fields of study. The goal of switching from traditional testing methods to oral examinations led to preserving academic integrity. Moreover, the results show that oral examinations improve the interaction between faculty and student. The experiment occurred during the quarter term of 2021, during which the form of instruction was remote. The examination consists of questioning the student in an interrogative manner via Zoom video conference. Three surveys serve as evidence to measure the effectiveness using the Likert scale. During the pre-exam study, data shows that students had no previous experience with oral examinations. However, studying for an oral examination strengthens the technical speaking skills of the student. The results proved that oral examinations are an effective method to promote academic integrity while also helping to raise student engagement.

Phillip Dawson (2015) discusses five different types of attacks against e-exams. The first type of attack involves copying the content of the USB drive into the student's hard disk. The second type of attack consists of the use of virtualization software. Most proctoring solutions nowadays have the functionality to detect instances of virtualization. However, some workaround may enable the student to load the contents of the exam into a virtual machine. The third type of attack is by using a USB key injector. A USB key injector is available at a reasonable price in many online stores, and the student customizes the functions. Finally, the fifth method to defeat BYOD e-exams is creating a memory dump and storing the file on the hard disk (Dawson, 2015).

The University of the Philippines Open University surveyed 52 students enrolled in the Master of Information System program. The survey consisted of three questions concerning academic dishonesty. Research shows that academic dishonesty is challenging for face-to-face and online courses (Ravasco, 2012). Although, the results showed more instances of academic dishonesty in face-to-face classes. Several factors, such as achieving a higher rank among classmates, reducing the time of the study materials, and being able to find a job, are among the reasons why students decide to cheat. Some suggested ideas are using a search engine, copying and pasting questions into the search engine, creating custom scripts, and running unauthorized processes. Others told the concept of hacking the university portal.

Moore et al. (2017), from the University of Tennessee, talk about how Respondus Lockdown Browser has shown not to be enough for online exam proctoring. Although Respondus also allows the instructor to activate the Respondus Monitor for each exam. Webcam testing with Respondus was not part of the pilot program, but the evidence shows screenshots of students being able to cheat with this application. The recommendation is to use remote proctoring, which may turn expensive for the average community college student. Besides relying solely on online proctoring, they also recommend strategies such as showing only one question at a time, changing the wording on the publisher's test banks, adding a letter to each answer choice, and protecting access to the examination with an access code.

Moten et al. (2013) present online cheating methods, such as waiting for answers, fraudulent error messages, collusion, and essay plagiarism. In distance education courses, instructors give the flexibility to take an assessment. Some students wait until others have an opportunity to take an exam to get the answers (Moten et al., 2013). Other students, who are not preparing for the examination, will try to preview the assessment and produce a fraudulent message. Moreover, students may also choose to provide login credentials to another individual. Furthermore, they discuss methods to prevent academic dishonesty in an online environment.

Policy dissemination, surveillance, proctoring, and statistical analysis are some countermeasures effective in preventing cheating.

Diedenhofen and Musch (2016) developed PageFocus, a new JavaScript that can detect and prevent cheating on unproctored internet tests by registering whether test takers abandon the test page by switching to another window or tab. In addition, a second function displays a pop-up as a warning message for the student. The implementation leads to the observation that students need at least three seconds to cheat on a question. In addition, PageFocus revealed that participants cheated when performance-related incentives were given (Diedenhofen & Much, 2016). The software is available for distribution on GitHub at the time of this writing. While it may be a valuable resource for proctored assessments, not all computer systems can run JavaScript.

Sullivan (2016) suggests alternative strategies to proctoring solutions. His integrated approach focuses on quiz design techniques to preempt cheating. Presenting students with multiple versions of the quiz, allowing multiple attempts, using a variety of question formats, and quiz frequency are among the recommendations. Nowadays, most learning management systems offer built-in features like the ones discussed. The findings confirm that technology tools, such as randomizing questions, shuffling response sets, and monitoring timestamps, reduce expectations that cheating pays off (Sullivan, 2016). Relying solely on quiz features may not be an option for other institutions, as protecting the integrity of online assessments is a requirement for accreditation agencies (Southern Association of Colleges and Schools Commission on Colleges, 2018).

Alessio et al. (2017) examine the effects of proctoring on online test scores. The scores of proctored examinations with webcam recordings are significantly lower than none proctored examinations (Alessio et al., 2017). Students who take the proctored exam with webcams are less likely to access unauthorized testing materials and commit academic dishonesty. Moreover, students who tested with lockdown software and no webcam recording had less impact on grading. Lockdown Browser and Secure Software offer several options for proctoring online exams. Both technologies assisted faculty with the review process. However, reviews are only based on abnormalities and do not cover issues of impersonation or unauthorized alterations of the testing software.

Definitions & Tools

Definitions

- Artificial Intelligence or AI – The theory and development of computer systems that perform tasks typically requiring human intelligence, such as visual perception, speech recognition, decision-making, and translation between languages (Lexico, n.d.a).
- Impersonation – Pretending to be another person for entertainment or fraud (Lexico, n.d.b).
- Automated Proctoring – The recording of online test takers at the assessment time. Usually with a third-party application or browser plug-in. The footage is generally available for review twenty-four hours after the last submission (if multiple submissions are allowed).
- Remote Desktop – Accessing a computer system from a distance. For this research, remote desktop means granting access to the test-taker system before an exam.

Another person will take control of the mouse and keyboard remotely. Details of this technique and how it allows impersonation are described in the methodology section.

- Executable File – A file or program can be run by a computer (Lexico, n.d.c).
- Executable file Analysis – The process of exploring the internal structure of the executable file. This technique is crucial for static malware analysis. We can see how the program will behave by looking into the resources table without loading the application into memory.
- Vulnerability – The process of exposing, finding, or exploring flaws within the application. The term is also common for other areas of cybersecurity. However, we are probing for vulnerabilities within the proctoring software.
- Virtual Webcam – The term virtual means that the product does not exist physically. Instead, we are replacing the existence of the hardware with simulation software.

Tools

- Respondus Lockdown Browser – We are choosing Respondus Lockdown Browser as the target for our experiment. The solution is currently in use by 1,500 institutions (Respondus, n.d.). The cost varies per number of students using the platform, which makes it affordable for institutions that choose to absorb the proctoring cost for the student. Additionally, it integrates seamlessly with Blackboard, Brightspace, Canvas, Moodle, Sakai, and Schoology. Moreover, we present working methods to bypass Respondus Monitor, the non-proctored add-on of Respondus Lockdown Browser.
- Windows Remote Assistance – Windows Remote Assistance is a tool included in recent releases of Windows OS. It does not require special licensing, is free to use, and is mainly intended to let someone fix a Windows computer system from a distance (Microsoft, n.d.).
- CFF Explorer – This application includes tools that might help reverse engineers and programmers (Pistelli, 2012). We will conduct executable file analysis with File Walker, a tool included within CFF explorer.
- e2eSoft Vcam – The application offers a wide variety of uses. However, we are using Vcam to install our virtual camera, and stream pre-recorded footage to our exam session with Respondus Monitor enabled (vcam, n.d.).
- FreeCam8 – Screen Capture software that remains undetectable by Respondus Lockdown Browser.
- A different computer system – Optional for optimal simulation results. Respondus Lockdown Browser disables any secondary displays; it is best to try Windows Remote Assistance and Quick Assist with another physical system.

Methodology

Our experiment proves the concept that instructional technology applications, specifically automated proctoring solutions with browser lockdown capabilities, are not safe from vulnerability researchers and bad actors. Our approach simulates the mindset of a student with a high determination to cheat, regardless if there is some motivation behind it. Exploring methods to break or bypass the multiple restrictions of proctoring software is limited. Some instructions are outdated in web forums and public video platforms. Therefore, we present modern working methods on how an online student can void the functionalities of proctoring applications. While our intention is not to promote academic dishonesty, it is vital to bring awareness to this matter.

Impersonation

First, we expose how the student version of the Respondus Lockdown Browser fails to detect instances of remote desktop software running as a process in our system. We must mention that a warning message will appear for every function that may assist the student while taking an exam. Also, the application can detect commercial software, such as Teamviewer. A student determined to cheat will plan days ahead of the examination. The process to start Windows Remote Assistance is simple. The student may invite a friend, classmate, or family member to take the exam on their behalf. This type of aid is fraud or impersonation, and no knowledge of network configuration, such as IP or MAC addresses, is needed. We start by creating an invite file and sending the file to the other end by e-mail. Then, we provide the session password to the test taker and grant complete control of the mouse and keyboard. Once the other person is in power, the student can launch the Respondus Lockdown Browser and enter login credentials into the learning management system.

Exploring for Flaws and Vulnerabilities

Respondus Lockdown Browser includes built-in functionalities to block features such as keyboard combinations, access to more than one screen, access to third-party websites, and other applications that are not authorized while a test is in progress. However, the application displays a “Loading...Please Wait” message before the institution’s landing page. An in-deep look with CFF Explorer and File walker shows the system files and functions used by Respondus Lockdown Browser. Our experiment reveals that we can use keyboard combinations and take advantage before the application loads all the necessary system components into memory. A significant discovery with this technique is that Respondus Lockdown Browser blocks secondary displays by opening a second application with a purple background, which blocks all other monitors except our primary display. Pressing the ALT + TAB key is typical in Windows Systems to switch between applications. However, we discover that it takes between zero to three seconds for Respondus Lockdown Browser before it blocks all attempts to launch applications. Pressing the ALT + TAB key during “Loading...Please wait” allow us to cancel the application that blocks secondary displays, and we can have full access to any material we may need to search for test answers.

Unblock A Secondary Display and Use Lecture Notes

A secondary alternative to null the efforts of blocking the secondary display is by doing a left click on the purple blocking window and pressing ALT+F4. Respondus utilizes two windows when a secondary display is in use. The first window is our exam session, which we use to authenticate to the LMS and take the exam. On the other hand, the second window serves as a blocking mechanism to disable a second monitor. However, it is possible to have a full view by closing the window with the key combination. Now, any click outside the testing window will result in a warning. After a second warning, the session ends and sends a report to the instructor. However, we need the secondary display to read notes only. We make this possible by inserting our lecture notes into a Windows 10 gadget named ‘Sticky Notes. To our surprise, we can start a Respondus session, and Sticky Notes can remain running as a background process without warning and any detection by Respondus Lockdown Browser. Therefore, it is possible to have lecture notes available, although the course instructor may not allow the use of notes.

Leak exam Content Via Screen Capture or Streaming

Respondus Lockdown Browser claims that it does not allow screen-sharing sessions while an exam is in progress. However, our extensive testing showed that Respondus could only block a limited set of applications that would enable the student to record the exam. Through extensive testing of applications, we found Free Cam8, a desktop capture software that goes undetectable by Respondus. Therefore, the use cases are almost endless once the student can utilize a screen capture application. We can start by saving the video and sending it through a third-party group chat like WhatsApp. Moreover, another alternative is to stream the video footage via a private link using YouTube or Google Drive. With the methods previously mentioned, a student can leak the content of any assessment by providing actual footage of the session.

Virtual Webcam and Pre-recorded Exam Footage

In most cases, instructors start the course with an ungraded practice quiz. It allows the student to prepare the system with any requirements and become familiar with the testing software. However, this also gives ample time for the student to develop a strategy and cheat without any red flags. After installing VCam, we set up a virtual camera with the intention of submitting an exam with pre-recorded footage. We can identify and time all the pre-exam steps by taking the pre-exam. Respondus Lockdown Browser has a sequence of steps, including taking a student picture, performing a 360-environment scan, showing a valid ID to the camera, and recording five seconds of audio and video. Our experiment shows that it is possible to submit an exam with footage that is not live. In other words, we recorded a session with enough time to pass the pre-exam screen successfully. Students may record footage for an extended period to mimic an entire session. Most learning management systems will display the time limit as part of the exam instructions.

Results

Figure1: Windows Remote Assistance (Test taker view).

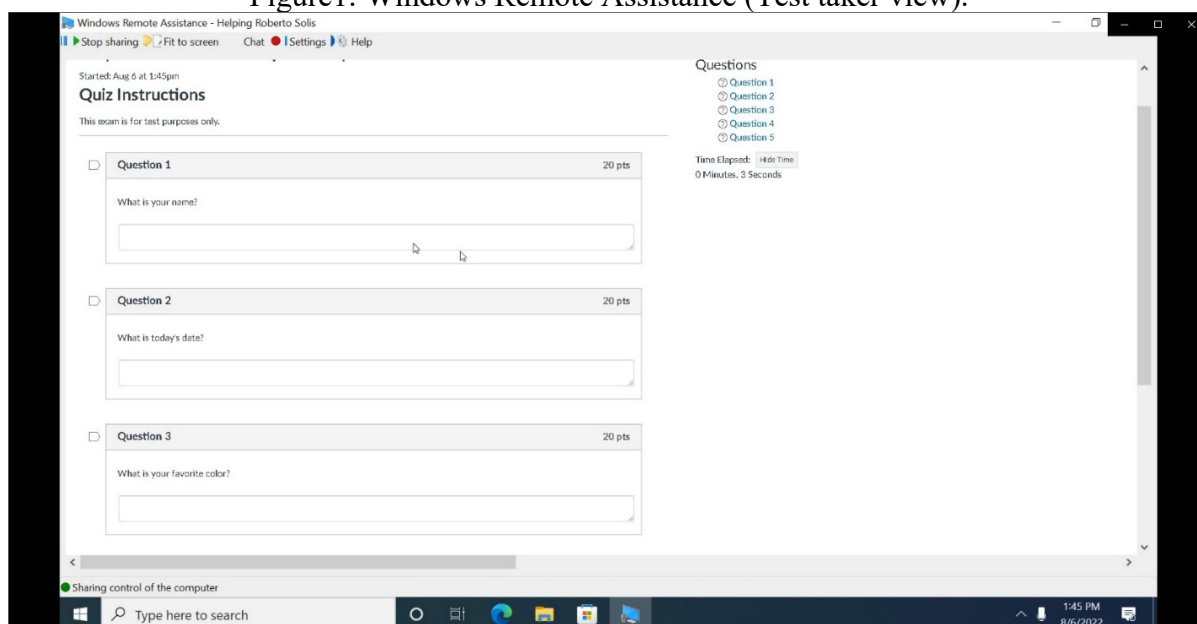


Figure 1 displays the remote test taker assisting the student with the exam. This is the impersonation method, where the student sends an invitation file to the test taker, and the remote user can request complete control and take the examination on behalf of the student.

Figure 2: Finding flaws using CFF File Explorer.



Figure 2 illustrates an in-depth look at the file structure of the Respondus Lockdown Browser. The application allowed us to examine what was happening in our Windows 10 system once we launched Respondus Lockdown Browser into memory. This specific method proved that the Respondus Lockdown browser only uses a secondary purple window to block a system with a dual monitor configuration.

Figure 3: Respondus Lockdown Browser blocking access to a secondary display.



Figure 3 presents how Respondus Lockdown Browser utilizes two screens when detecting dual monitors. The first monitor on the right side is the student’s view of the examination. Ideally, we are under the impression that we cannot use external resources during an

examination. We can see how a purple window is launched on the secondary display, which is located on the right side.

Figure 4: Answering questions on behalf of the student with Quick Assist.

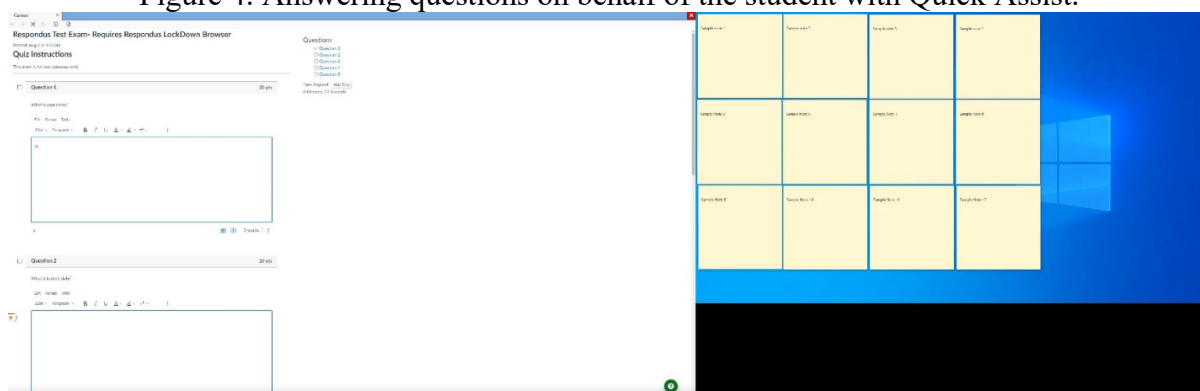


Figure 4 shows one of the major security flaws built within the Respondus Lockdown Browser. This example eliminates the blocking mechanism that disables our secondary monitor. We achieve this by pressing ALT+F4 on our keyboard. Also, we are under the impression that students cannot utilize external resources. This preview shows how Respondus fails to identify that Sticky Notes is running as a background process. As a result, the student can access lecture notes and take advantage of this significant security flaw.

Figure 5: Preview of our output file used to distribute and leak assessment content.

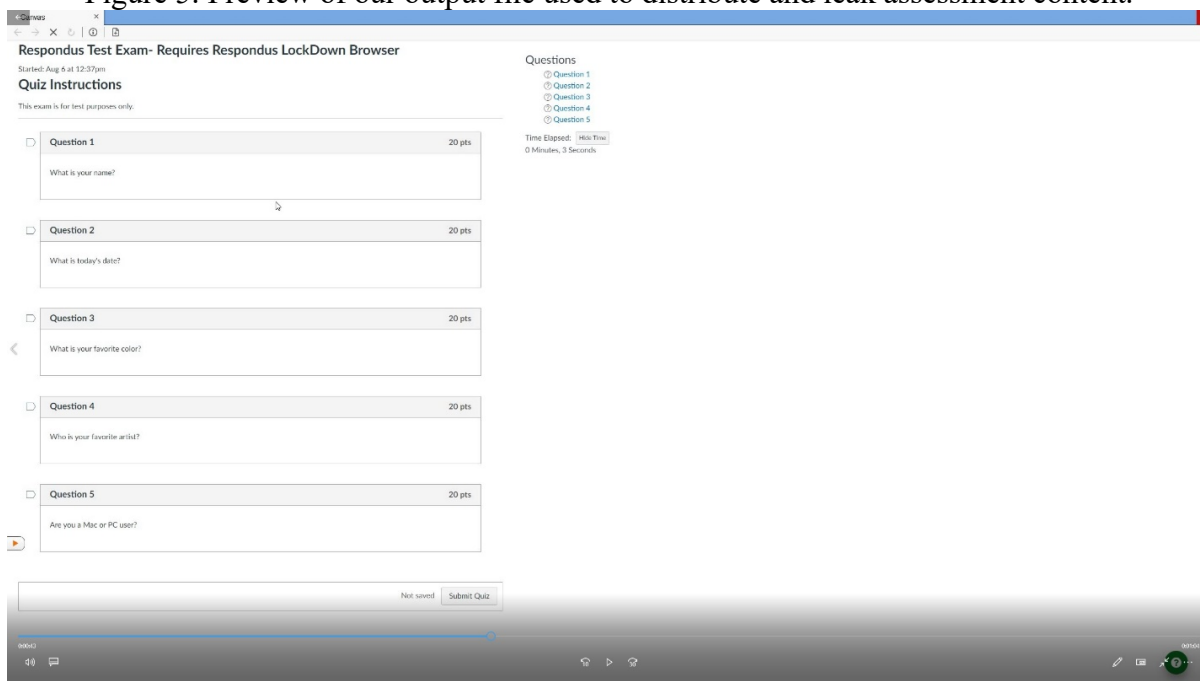


Figure 5 presents our output file that resulted from the screen capture experiment. A closer look to figure 5 displays the playback controls at the bottom. Once a video file is generated, a student can have multiple options to leak examination content into several group chats or use a private link to disburse the content among classmates.

Figure 6: Loading a prerecorded video to VCam.

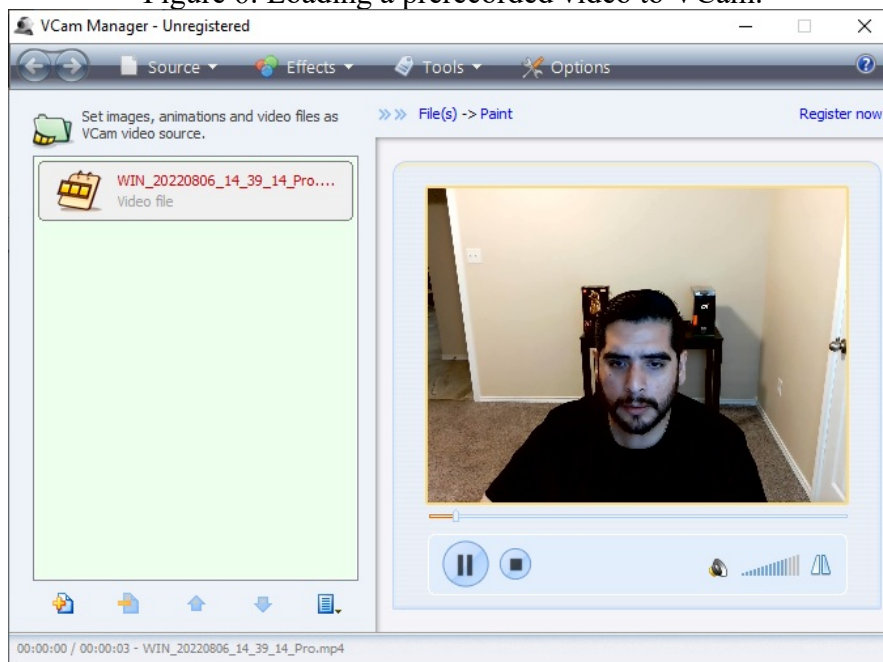


Figure 6 shows how we can use a webcam with Respondus Monitor. Here, we can load prerecorded video footage. The advantage of this method is that it eliminates the need to be recorded live when taking an assessment. Moreover, the most distinct feature is allowing the student to use any external device such as a tablet or laptop. Remember that this will not be shown to the instructor because the footage has been pre-recorded.

Figure 7: Using Vcam to take our assessment.

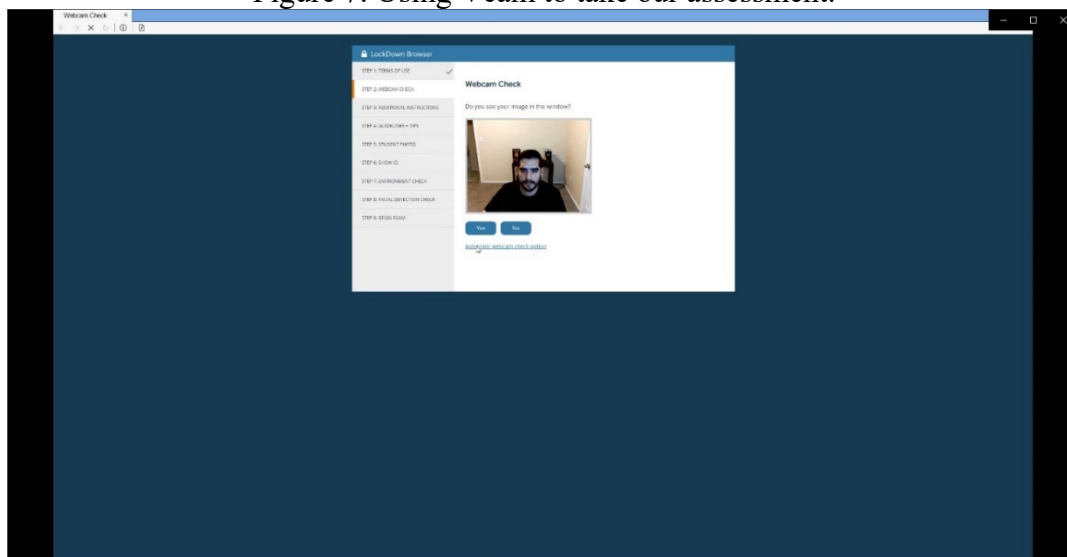


Figure 7 shows how we utilize a virtual webcam with a prerecorded video to take our assessment. Also, it is possible to bypass the webcam check sequence by following the pre-exam webcam check. Moreover, we can also utilize a video that covers the entire session. For example, an exam with a time limit of one hour will require a pre-recorded video of one hour.

Conclusion and Future Work

Our simulations prove several effective methods to assist a student, even when a security mechanism is in place to prevent academic dishonesty. In this case, we lure several security features built-in the Respondus Lockdown Browser. Windows Remote Assist allows an external person to take an examination on behalf of the student. This impersonation method works best when the exam only requires Lockdown Browser with no webcam. On the other hand, we explore the executable file to get an in-depth idea of the security mechanisms. This method allowed us to identify the blocking mechanism of a secondary display. Furthermore, we demonstrated how to bypass the mechanism that blocks a dual monitor configuration and take advantage of external resources such as lecture notes. We explore the endless possibilities that may result once a student uses video capture software to leak examination materials. Finally, we also exhibit how to lure and prevent a live recording of a student while an examination is taking place. We sincerely invite anyone in the academic community to keep testing which applications and methods are not currently detected by your proctoring solutions used in other institutions. We know Respondus Lockdown Browser has been in the market for several years and several institutions commonly utilize it.

References

- Alessio, H. M., Malay, N., Maurer, K., John, B. A., & Rubin, B. (2017). Examining the effect of proctoring on online test scores. *Online Learning, 21*(1), 146–161. <https://eric.ed.gov/?id=EJ1140251>
- Cai, H., & King, I. (2020). Education Technology for Online Learning in Times of Crisis. *2020 IEEE International Conference on Teaching, Assessment, and Learning for Engineering (TALE)*. <https://doi.org/10.1109/tale48869.2020.9368387>
- Dawson, P. (2015). Five ways to hack and cheat with bring-your-own-device electronic examinations. *British Journal of Educational Technology, 47*(4), 592–600. <https://doi.org/10.1111/bjet.12246>
- Diedenhofen, B., & Musch, J. (2016). PageFocus: Using paradata to detect and prevent cheating on online achievement tests. *Behavior Research Methods, 49*(4), 1444–1459. <https://doi.org/10.3758/s13428-016-0800-7>
- E2ESoft. (n.d.). *VCam – Easy to Enjoy*. Retrieved July 20, 2022, from https://www.e2esoft.com/vcam/#google_vignette
- E2ESoft. (n.d.). *Free Cam – Free Tool for Creating Screencast*. Retrieved July 20, 2022, from <https://www.freescreenrecording.com/>
- Küppers, B., Kerber, F., Meyer, U. & Schroeder, U. (2017). Beyond lockdown: Towards reliable e-assessment. In *Lecture notes in informatics* (pp. 191–196). Gesellschaft für Informatik.
- Lexico. (n.d.a). Artificial intelligence. In *English Dictionary, Thesaurus, & Grammar Help*. Retrieved July 20, 2022, from Lexico Dictionaries: https://www.lexico.com/definition/artificial_intelligence
- Lexico. (n.d.b). Impersonation. In *English Dictionary, Thesaurus, & Grammar Help*. Retrieved July 20, 2022, from Lexico Dictionaries: <https://www.lexico.com/definition/impersonation>
- Lexico. (n.d.c). Executable file. In *English Dictionary, Thesaurus, & Grammar Help*. Retrieved July 20, 2022, from Lexico Dictionaries: <https://www.lexico.com/definition/executable>
- Lubarda, M., Delson, N., Schurgers, C., Ghazinejad, M., Baghdadchi, S., Phan, A., Minnes, M., Relaford-Doyle, J., Klement, L., Sandoval, C., & Qi, H. (2021). Oral exams for large-enrollment engineering courses to promote academic integrity and student engagement during remote instruction. *2021 IEEE Frontiers in Education Conference (FIE)*. <https://doi.org/10.1109/fie49875.2021.9637124>
- Microsoft. (n.d.). *Use Remote Assistance to let someone fix your PC*. <https://support.microsoft.com/en-us/help/4026516/windows-use-remote-assistance-to-let-someone-fix-your-pc>

- Moore, H., Derrick, H. J., & Griffin, R. B. (2017). Impeding students' efforts to cheat in online classes. *Journal of Learning in Higher Education*, 13(1), 9–23. <https://eric.ed.gov/?id=EJ1139692>
- Moten, J., Fitterer, A., Brazier, E., Leonard, J., & Brown, A. (2013). Examining online college cyber cheating methods and prevention measures. *Electronic Journal of E-Learning*, 11(2), pp139-146–pp139-146. <https://academic-publishing.org/index.php/ejel/article/view/1664>
- Pistelli, E. (2012). *Explorer Suite*. NTCore. https://ntcore.com/?page_id=388
- Ravasco, G. G. (2012). Technology-aided cheating in open and distance e-learning. *Asian Journal of Distance Education*, 10(2), 71–77. <https://www.learntechlib.org/p/185226/>
- Respondus. (n.d.). *Lockdown browser*. Retrieved July 20, 2022, from <https://web.respondus.com/he/lockdownbrowser/>
- Sullivan, D. P. (2016). An integrated approach to preempt cheating on asynchronous, objective, online assessments in graduate business classes. *Online Learning*, 20(3), 195–209. <https://eric.ed.gov/?id=EJ1113346>

Contact email: rds050@shsu.edu
nks001@shsu.edu
cxv007@shsu.edu