DIGITAL EXAMINATIONS: MITIGATING THE RISK OF STUDENTS GETTING OUTSIDE HELP WHILE TAKING AN ONLINE EXAM

Matteo Iannizzotto, Senior Software Engineer @ Murex and Adjunct teacher in Digital innovation, Microsoft Excel and Algorithmic thinking & programming structures @ IESEG

Abstract

The advent of the Fourth Industrial Revolution has triggered profound global changes. Data abundance, unprecedented computing power, ubiquitous connectivity, and advanced algorithms have revolutionized daily activities such as transportation, dining, shopping, and even academic assessments. Schools have embraced digitalization by transitioning exams from paper to computer, offering benefits like environmental sustainability, error reduction, quick grading, and indefinite record-keeping. However, this shift also introduces challenges, such as the risk of students cheating by exploiting the accessibility of digital resources. This chronicle proposes a simple yet effective solution to mitigate cheating while maintaining the advantages of digital exams over traditional paper-based assessments.

Key-words: digitalization – cheating – Generative AI – digital examinations

Résumé

L'avènement de la Quatrième Révolution Industrielle a provoqué des changements mondiaux profonds. L'abondance des données, la puissance de calcul sans précédent, la connectivité omniprésente et les algorithmes avancés ont révolutionné les activités quotidiennes telles que le transport, les repas, les achats et même les évaluations académiques. Les écoles ont adopté la numérisation en transitionnant les examens du papier à l'ordinateur, offrant des avantages tels que la durabilité environnementale, la réduction des erreurs, la correction rapide et la conservation indéfinie des copies. Cependant, ce changement présente également des défis, tels que le risque de tricherie des étudiants en exploitant l'accessibilité des ressources numériques. Cette chronique propose une solution simple mais efficace pour atténuer la tricherie tout en maintenant les avantages des examens numériques par rapport aux évaluations traditionnelles sur papier.

Mots-clés : numérisation – tricherie – Intelligence Artificielle Générative – examens numériques

Cheating tendencies during online examinations

The advantages of digital examinations are undeniable: less environmental waste, reduction of risks in the implementation chain (printing out the wrong – number of – copies, mixing up students, losing papers…), mitigation of human mistakes (wrong grading, assessment misreading…), correction efficiency (hundreds

of copies can be corrected in few seconds) and redistribution (feedbacks can be sent to students immediately after the correction), as well as the possibility of keeping records potentially forever.

But let's be honest; allowing a student to use their personal laptop, connected to the Internet, also means giving them the possibility to cheat:

- It's easy to take screenshots of the exam, to later give / sell them to other students.
- It's feasible to send the questions to someone else and get help on the answers (via WhatsApp, e-mail, Instagram…)
- Since the end of 2022, the student can also get help through one of the Generative AI tools such as ChatGPT or Bing Chat.

Even with measures like question randomization, frequent updates to question banks, strict penalties for cheaters, and invigilated exams, many students still find ways to cheat, both actively and passively, to some extent.

New strategies are essential to ensure students remain continuously present on the examination screen, preventing them from taking screenshots or sharing questions with unauthorized individuals.

Intercepting focus loss: the *blur* event on web browsers

Assuming that digital examinations typically occur within a web browser, and most web pages operate under the assumption of JavaScript being enabled, an event listener can be utilized to execute a piece of code whenever the user navigates away from the current browser window:

```
window.addEventListener('blur', function() {
    'POST on server: focus loss from time A to time B
});
```

Consequently, if the exam webpage includes such an event listener registered within its current window, the student would be unable to shift focus away from it. This prevents actions like taking screenshots or sending messages outside of the exam page, as the browser would intercept such events and execute the function associated with losing focus.

A potential solution to safeguard digital exams from cheating attempts involves creating a simple web application comprising:

- A front-end component featuring an *iframe*[1] displaying the exam webpage (e.g., Moodle, WiseFlow) and an event listener for the *blur* event. This listener notifies the back end whenever the *blur* event occurs.
- A back-end monitoring system that tracks student activity, enabling the detection of any periods of inactivity on the exam webpage.

The diagram below illustrates the sequence for a single student:

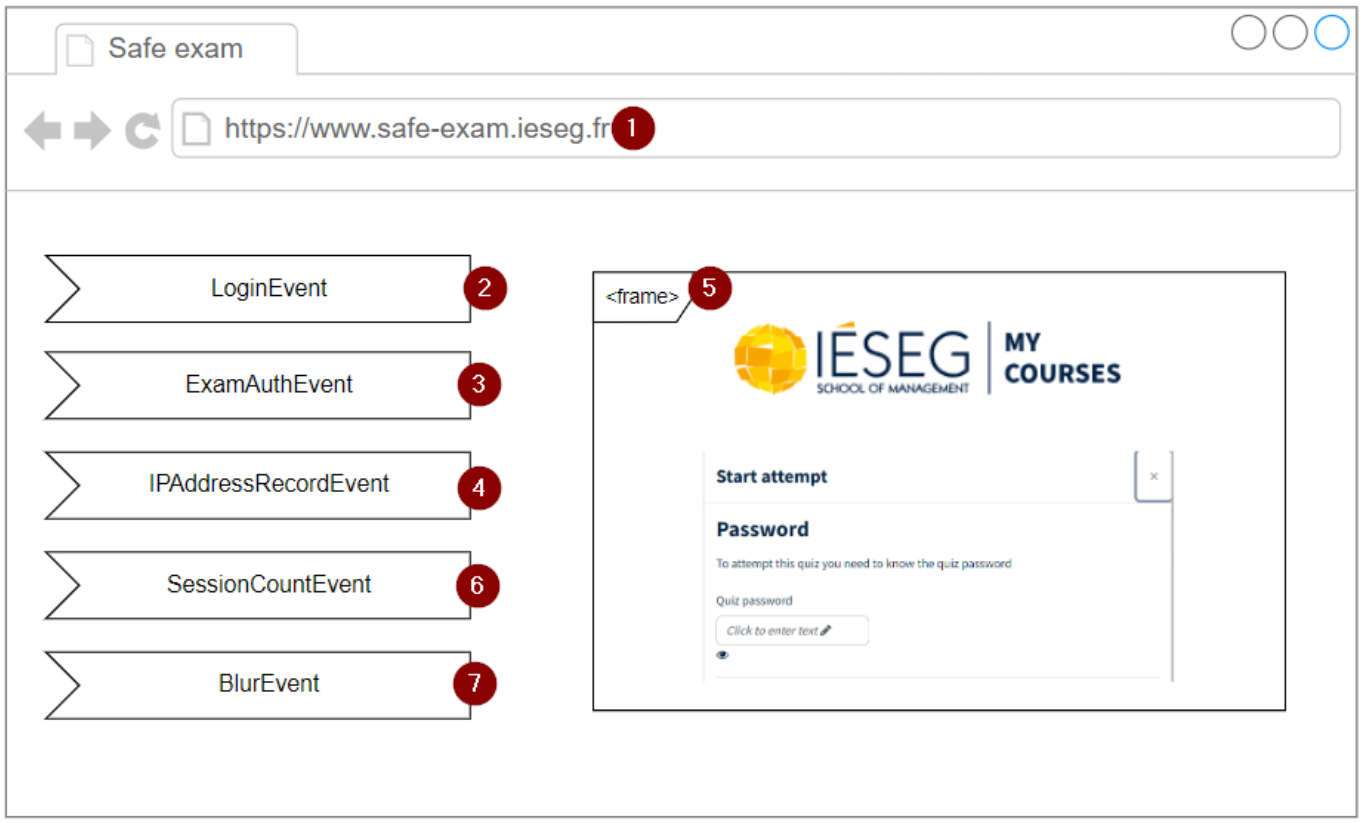

Figure 1: simplified sequencing of the "Safe Exam" framework

Based on Figure 1, the step-by-step sequence is as follows:

1. The student accesses a URL to open the safe-exam application.
2. The student logs in using standard authentication to access the examination platform, with the backend recording this login event in the database (including student username and timestamp) and storing the full token in the browser's local storage for platform authentication.
3. The web application prompts the student for a password to authorize connection to the platform, generated by the application and associated with the current examination. Invigilators provide this password to ensure only the student can connect.

[1] An iframe is an integrated element of the HTML document that allows to display the content of another website within the same page

4. The backend records the student's current IP address in the database along with their username and timestamp.
5. The student is redirected to an iframe containing the digital exam, such as a Moodle quiz.
6. The backend monitors the number of open sessions for each student, ensuring it remains consistent with standard examination protocol.
7. Whenever the blur event occurs, the webpage sends a message to the backend indicating whether the session (student username + student IP address + examination authorization) has lost or regained focus on the webpage.

Rebuilding the student activity for a given examination

In a legitimate sequence for a digital examination for a student X, there should be a single exam authentication from a known IP address (associated with the school premises), for a single session that maintains focus on the webpage without any recorded blur events during the examination timeframe.

Considering the primary key for an examination as the combination of student username, student IP address, and examination ID, the following cheating attempts can be readily identified:

a. If the student attempted to switch pages on their own laptop, regardless of the reason, a blur event would trigger and post a message indicating the loss of focus from time A to time B on the server.
b. If the student enlisted someone outside the school to take the exam for them and communicated the exam password, two sessions from different IP addresses would be recorded for the same examination, indicating simultaneous exam attempts by two individuals for one person.
c. If the student solicited someone inside the school to take the exam for them, although both sessions would share the same IP address, the system would still detect multiple sessions for the same examination.

Certainly, students should be made aware of the system in place to monitor their exam activity. It's in their best interest to refrain from leaving the examination webpage for any reason to avoid being flagged as cheaters. This emphasizes the importance of maintaining focus and integrity throughout the examination process.

Limitations and possible mitigations

The proposed solution does have limitations, but there are potential mitigations available.

Limitation	Mitigation
The student may disable JavaScript on their browser to avoid being intercepted from the *blur* event listener	The web application can be notified on JavaScript disabling and consider this as a cheating attempt as well
The student may connect to the platform to register for an examination session, but ask someone else to realize the examination directly on the target platform	Most platforms do not allow multiple sessions to be open on the same quiz (for example Moodle or WiseFlow). But even if it was the case, another listener can be added to detect inactivity (i.e. how long does the user spend on typing/scrolling the page)
The student may legitimately need to abandon the examination page (e.g. to go to the restroom)	An invigilator button can be added (and protected by an admin password) to stop the blur events from triggering during that timeframe

Conclusion

With this straightforward proposal, digital examinations can be implemented for most exams with minimal cheating risk. Although there would be some time required for platform development and beta-testing, the system would quickly become flexible enough to facilitate web-based exams while preserving their advantages. The next phase would involve further development to enable exams to be conducted on local applications such as Microsoft Excel, Matlab, R, etc.

Bibliography

All the content of this article is the result of the writer experience as a software engineer and adjunct teacher of technological subjects. For a deeper reading of the *blur* event and the *iframe* mentioned as part of the proposed solution, the following links can be consulted:

- Blur event: https://developer.mozilla.org/en-US/docs/Web/API/Element/blur_event
- iframe element: https://developer.mozilla.org/en-US/docs/Web/HTML/Element/iframe