Performing Computer Science Examinations in a Fully Online Environment

Atanas Semerdzhiev[0000-0002-7760-1619], Dimitar Dimitrov[0000-0002-6806-9501], Nora Angelova[0000-0003-2697-9766], Petar Armyanov[0000-0002-4903-8945], Trifon Trifonov[0000-0002-2247-1968], and Kalin Georgiev[0000-0002-6283-1040]

Department of Computer Informatics, Faculty of Mathematics and Informatics, Sofia University "St. Kliment Ohridski", Bulgaria

{asemerdzhiev, dgdimitrov, noraa, parmyanov, triffon, kalin}@fmi.uni-sofia.bg

Abstract. Since the advent of the COVID-19 pandemic the Faculty of Mathematics and Informatics of Sofia University "St. Kliment Ohridski", similarly to many other educational institutions, was compelled to transfer the entirety of its educational activities online. This raised significant challenges to the performing of exams in Computer science and Software engineering. This article summarizes our method for conducting exams online. It describes the challenges faced, security risks identified, and what was done to mitigate them. We propose a method for conducting exams resulting from our experience. The results described in the article reflect the experience of more than 15 teaching and examination teams led by the authors with more than 1000 students over the period of April 2020 – April 2021.

Keywords: Education, Exam, Security, E-learning, COVID-19, Sofia University, Computer Science, Software Engineering.

1 Introduction

Similarly, to virtually all educational institutions in the developed world at the advent of the COVID-19 pandemic, the academic staff of Sofia University's Faculty of Mathematics and Informatics ("FMI") was compelled to transfer swiftly all of its educational activities online. One of the activities most significantly impacted by this change was the conducting of exams in subjects related to Computer Science ("CS") and Software Engineering ("SE").

In Bulgaria, the COVID-19 pandemic triggered a process of transferring all educational activities to an online environment only three weeks after the start of the summer 2019/2020 semester. As a result, all classes were immediately migrated to an online environment. The swift change allowed no time for careful deliberation and analysis of the available methods of performing exams online, although valuable experience was quickly accumulated with teaching activities

and the students' readiness to participate efficiently in the educational process online. While it was impossible for the teams teaching CS/SE to forecast the duration of the pandemic, we planned for the worst-case scenario, namely that there will not be an opportunity for a face-to-face encounter with the students throughout the end of the academic year. This assumption proved largely correct, despite a limited reopening, which allowed in-person examination to take place at the faculty under a set of restrictions. Our goal was to create collaboratively a model for conducting examinations that could be applied in a fully online setting.

Throughout the course of the semester, we had the opportunity to experiment with alternative versions of a model for performing midterm exams, thus identifying opportunities for improvement. This experimentation was done with the understanding that the new models inevitably introduce obstacles that objectively prevent students from demonstrating their skills and abilities properly, and the team was prepared to grade in favor of the students whenever such issues were identified.

This article is focused on our proposed method for conducting examinations in CS/SE subjects online. It describes the challenges which were (and are still) being faced, the security risks which were identified, and what was done to mitigate them, ultimately establishing a stable model for conducting examinations fully online.

2 Problem statement

Let us first establish the kind of exams that will be discussed in this article and to which our model is intended to apply. The exams in question are in the field of Computer Science and Software Engineering and evaluate the students' problem-solving abilities with the use of a specific programming language (in our case: C++, Haskell, and SQL). Exams in these subjects are typically of short duration, usually between 1 and 4 hours. At the beginning of the exam, the students receive one or more problems that they are required to provide a solution. For example, students may need to create a computer program as a solution to the exam problems. In other situations, students are not required to implement an entire program, but a single class, or a single function, or a combination of such program units. Each student solves the exam on their own, using a computer with preinstalled IDE, compiler, etc. At the end of the exam, each student submits their work in the form of one or more source files. Submissions are uploaded to FMI's e-learning system, which is an instance of the popular LMS platform Moodle [1]. It should be noted that the above describes the mechanics of in-person examinations, but all these aspects are perfectly applicable to a fully online environment and provide an excellent starting point.

While designing our model, we identified several goals that it should achieve, as listed:

- **fully online** – all aspects of the examination should be conducted online without any physical interaction;
- **fair –** should provide the students with as equal opportunity as possible to demonstrate their skills and abilities;
- **resource efficient** – the model should not impose an undue resource constraint on neither the students, nor the examination staff, taking into account that both use their personal devices and personal accommodation for the conducting of the exam;
- **technology agnostic** – should not impose requirements for a specific hardware or software platform;
- **fault-tolerant** – should allow for a limited number of technical failures without sacrificing the validity of the exam;
- **auditable** – should allow for an independent audit of the examination process and independent grading of the students' performance;
- **familiar** – should not differ drastically from the in-person examination; and
- **secure** – should provide a balanced set of measures against cheating and any forms of unfair behavior by the students in general.

3 Challenges and constraints

Traditionally, exams at the FMI are conducted in a controlled environment. The students enter a room, where each working place is equipped with a computer configured in a standardized manner. This has several benefits including:

- The examination staff has control over the configuration of the computers on which the exam takes place. This includes the list of installed packages, security settings, etc. In particular, this allows for setting up a specialized training or examination environment involving the integration of multiple systems, e.g., connecting different database management systems (cf. [2]).
- The students are admitted in the rooms where the exams take place only at a predetermined time. This limits their physical access to the machines and thus limits the opportunities for tampering with the computers before the exam. Since those rooms are shared between exams and used to carry out regular classes, it may be possible for an individual to gain physical access to a particular computer before an exam, but it is a much more complicated process, taking into account that they also have to be assigned to the same room and computer during the exam.
- One or more members of the examination staff are always present in the room where the exam takes place. They can assist the students if they have questions related to the exam, as well as help resolve technical prob-

lems with the IDE, OS, machine, network, etc. Additionally, they may closely monitor the activities of any student that take place during the exam at their own discretion.

- All computers are part of the same private network and connection to the Internet may be disabled during the exams.
- All smart devices must be switched off and stashed away in the students' bags, coats, etc. during the exam. If a student is found to use any type of communications device during the exam, he is automatically failed.
- Physical interactions between students during the course of the exam are strictly monitored at all times and are effectively restricted.
- The use of additional physical and electronic materials may be strictly controlled and effectively prevented altogether.
- Student identification is performed via a university-issued photo ID.

During the COVID-19 epidemic, as we were forced to take all our activities online, this entire setting changed. As many of our students started attending classes and exams from home using their own computers, we were now faced with the following reality:

- The examination team has little or no control over the configuration of individual computers. They may come preinstalled with all sorts of packages and their configuration cannot be controlled. This is not just a technical matter, but also a legal (and, arguably, also a moral) one, as our students have no formal obligation to follow additional rules on their personal computers.
- Each student is working on a different computer, with a different OS, etc., i.e., no standardized configuration is in place.
- Students are working on their own machines, it is natural that they have access to their machines 24/7 and can do with them as they please. This provides many benefits when participating in classes, as each person can configure their computer the way they see fit. However, this also raises significant risks about cheating and unfair behavior when it comes to exams. In particular, they have instant access to all course materials, especially when the course is conducted entirely online.
- Network access and setup at each location cannot be controlled. They also come in all sorts of different configurations.
- Any form of physical control by the examination team is practically impossible. In particular, it cannot be guaranteed that the students are not using additional materials, devices, or even the assistance of other people present in the room.
- The student may operate more than one device at the same time – e.g., be able to use his smartphone, another laptop, etc. while also working on the exam. This provides an opportunity for electronic communication

with an assisting person or another student that is difficult to establish and prevent.

Naturally, under those conditions, it is challenging to establish a safe environment in which to conduct exams. It may be argued to what extent it is possible at all.

It should be noted that, based on our experience, when students are determined to cheat, they usually find a way to do so. When this phenomenon becomes dominant, i.e., most of the students present in the classes do not seek to gain new knowledge and skills, but rather to formally gain an exam score and subsequently a diploma, then the entire educational process is compromised (a more detailed discussion on this topic may be found in [3]). It is extremely hard to accomplish any educational goals in such conditions. It is our belief that most of the efforts of educators should be focused in the direction of motivating students. Unfortunately, ensuring that students in a class are really after attaining a better qualification, instead of just "chasing a diploma" is not always possible and, understandably, anti-cheating mechanisms should be put in place. Our belief is that no such measure can be truly successful if the foundations of the educational process are not set properly. Moreover, more, if the students perceive the training as just a formality that must be checked off and the exam as a formal obstacle that must be passed at all costs, rather than as an evaluation, which is aimed to provide feedback on their work and skills, gained. This requires effort both on part of the teaching staff to establish a natural, humane, and just educational process and on the part of the students, who must come from a point of genuine desire to develop in a specific area, rather than just to receive a formal document.

That said, our experience shows that if no measures are put in place to prevent cheating and if it does not require an implicit intention and effort for such mechanisms to be avoided, this leads to an interesting phenomenon – even students, who would not normally cheat, start doing so. On the other hand, when at least some such mechanisms are put in place, students tend to show appreciation of the significance and consequences of their actions and restrain from unfair behavior. Therefore, our quest is to find a balance between a fully liberal system allowing complete freedom for students during and exam, and a system implementing strict barriers for disallowed behaviors.

4 Risks

In the conditions described above, there are many risks related to conducting exams. In this section, we list several of them.

4.1 Security of the facility in which the exam takes place

- In the room in which the student resides, while they take the exam, there may be other people. Their presence may not be announced, and they

may attempt to assist the student, or even perform all the work and let the student submit it as their own.

- In the room, there may be additional devices, which the student may use to assist him in the exam. Those may be other computers, smartphones, communication devices, etc. In one scenario, they may be used to connect him to another person, who will aid them during the exam. However, they may also be used to look up answers on the Internet, submit solutions to another student, etc.
- Although not related to the facility per se, such additional devices may be hidden on the student's body. Now of writing of this article, in the country of origin of the authors, it is possible to obtain a small "spy" earphone, which entirely hides within a person's ear and which can connect to a smartphone via Bluetooth at a price range of 30 – 75 EUR. Having in mind that such devices are also offered "for rent" during a limited period, this makes such a solution highly affordable. At the same time, it allows another person to wait in a room next to the one in which the student takes an exam and aid them. As any educator surely knows, such "cheating aids" present a significant problem in in-person exams as well. However, in the case of fully online exams, where the students attend an exam from a place of their choosing, they are virtually undetectable and the presence of people aiding the student cannot be established. Similarly, other devices can be obtained, which provide a reverse communication link from the student to potential aiders, to transmit auditory and visual information.

4.2 Security of the computer on which the student takes the exam

- On the computer on which the student takes the exam, there may be additional software used to assist them during the exam. In its easiest form, this may manifest as an open browser tab to look up answers on the Internet. Techniques that are more complicated are also possible.
- The student may provide network access to another person to log in to his or her computer via popular means such as an FTP server, Remote Desktop, etc. Those allow a remote user to connect to the computer on which the exam takes place and solve a given problem, leave files containing a solution, etc.
- The student may be running a hypervisor and through it – a guest virtual machine. They can take the exam from the guest OS, which enables them to run all kinds of packages on the host OS and those cannot be detected from the guest. This may neutralize anti-cheating tools such as the Safe Exam Browser [4].

Naturally, any or all of the above may be used in tandem. For example, in a programming exam, the student may take screenshots of the assigned problem. The screenshots may be automatically synced to a cloud account. Another person may retrieve them from there, solve the task and upload the solution back to the student's computer. The student can then submit the solution as his or her own. If carried out properly, this technique can be applied without showing any visual indications on the user's screen.

5 The examination model

Below we describe our model for conducting exams. It attempts to address the risks stated in Section 4, while solving the challenges described in Section 3 and meeting the goals defined in Section 2. In the process of developing and establishing this model, we were naturally forced to make many tradeoffs due to a variety of technical, legal, and moral issues. We admit that our model is far from perfect and may not be directly applicable "as is" in another setting. We aimed to rationalize each of its aspects by describing which issues are addressed by each measure. Finally, we also comment on issues are not yet addressed and remain open.

5.1 Examination environment

We allowed the students to use a computer, operating system, IDE, and network of their choice. We required that each student to be equipped with

- a stable and reliable internet connection,
- one of the four most popular web browsers (Chrome, Edge, Firefox, Safari),
- a working microphone and speakers or headset,
- a working camera, which can transmit video at an acceptable resolution and frame rate; ideally a **mobile** camera to be placed independently of the student's computer,
- a university-issued or state-issued photo ID.

The online environment for conducting the exam may be any videoconferencing software, which meets the following requirements:

- works in a web browser without the need for a separate installation, being able to operate on a mobile device is a plus, which makes it possible to use it as an independent mobile camera
- allows for simultaneous video and screen sharing by multiple participants
- allows for recording of the session
- allows for advance scheduling of the sessions

Our platform of choice was Google Meet [5], which was made available to educational institutions for free [6]. It was significantly improved over the

course of the COVID-19 pandemic. In particular, it satisfied all requirements stated above.

5.2 Examination plan

1. **Session scheduling.** Before the exam, we regenerate a meeting code for each student. This code allows them to access a separate virtual conference room, which we will refer to as an *examination room*. Each student receives a unique meeting identifier. Two variations are possible:

- no two students share the same examination room, or
- a limited number of students share the same examination room.

Each examiner is assigned to one or more examination rooms. Prior information about the students taking the exam may be used to control the assignment of students and examiners to room, e.g., to determine the optimal amount of examination rooms and students per examination room (in case they need to be shared), to ensure that students sharing an examination room are assigned different sets of problems, etc.

2. **Session setup.** On the day of the exam, all students enter their designated examination rooms. Members of the examination team also enter each of their designated rooms. One examiner enters multiple rooms (usually between 4 and 8) and is responsible for monitoring the students there. They can also respond to any questions that the students may have on the exam or address any technical issues occurring throughout the exam. The examiner verifies that each of the students has properly working microphone, speakers, and camera, which is properly placed, and ensures that no audio feedback is present (in case a second device is being used as the camera).
3. **Student identification.** Prior to the start of the exam, the examiner requests each of the student to present their identification document to the camera, such as an ISIC card, an official document from the university, etc. This is intended to prevent someone else posing as the student. This closely mirrors the manner in which the identification is performed in an in-person exam.
4. **Screen monitoring.** During the exam, students are required to share their entire screen (as opposed to just a browser tab or a window). This allows the examination team to monitor their activities with the device while working on the exam.

- If there is only one student in each meeting, this prevents any interaction of the student with other students. The disadvantage of this setup is that one examiner may only monitor as many students as the number of the examination rooms he can enter simultaneously.

- If several students share a room, then the examiner is also required to monitor all of the students' shared screens (usually tiled) so that they can determine if a student is looking at another student's shared screen. This is akin to an examiner monitoring the student's activities in an in-person exam. While more taxing on the examiner, this variation also allows more students to be monitored by the same examiner.

5. **Auditory and visual monitoring.** *Auditory monitoring* is performed via the student's microphone. Its activity may be tested at any time by the examiner by "pinging" the student via audio and requesting an auditory response. *Visual monitoring* is performed via the student's camera. Ideally, the standalone camera has to be placed to the side at an angle, so that the examiner can see simultaneously the area around the keyboard, the computer screen itself and its contents. This mimics, as closely as possible, the visual monitoring in an in-person exam by allowing the examiner to see at least part of the student's surroundings as well as their interaction with the computer. If a student has only an embedded camera that is not detachable, then he/she is advised to login to the conference room with its personal smartphone and use one of the cameras there. Since practically all students own smartphones, they are not obliged to buy any additional hardware such as external web cameras. As a last resort, if only an embedded camera is available, the student is asked to switch it on so that at least their face may be monitored by the examiner, but not the surrounding environment, or the physical interaction with the computer. Students are requested to keep their microphone, speakers, camera, and screen sharing active and switched on at all times. Failing to do so at any point in time is considered a fault, and multiple faults may result in exam failure for the student.
6. **Session recording.** The entire exam session is being recorded for auditing purposes. The recording is started only after the student identification is performed. This is for personal privacy reasons; so that the student personal ID document does not remain in the recording. The recording may be used for reexamining a student for suspicious behavior, as well as by an independent auditor of the examination, in case there are any questions regarding how the examination was conducted. Ideally, the recording is performed by the videoconferencing software, which also records timestamp information and prevents tampering, allowing the recording to be used as independent evidence for how the examination was conducted.
7. **Solution submission.** Students submit their solutions to a predesignated location, ideally an e-learning system such as Moodle. This process is monitored by the examiner to ensure that the submitted solution

matches the file on which the student has been working throughout the exam. This can be also verified later on the session recording. Ideally, the student is requested to signal his intent to submit a solution prior to doing so. The student is requested to announce their completion of the submission. After which he/she leaves the session and are noted by the examiner. Any unannounced room departure is considered as a fault. It may result in exam failure for the student.

8. **Plagiarism detection.** After the completion of the exam, all submissions are scanned with antiplagiarism software, such as JPlag [7] or Moss [8]. This measure is intended to detect cases where one student submits their work to another, who can submit it as their own, and this is not noticed by the monitoring examiner(s) [9]. Since the examination duration is limited, this leaves little time to introduce variety in the source code of the solution. Thus, plagiarized work is relatively easy to detect, as opposed to assignments in which the students have days, weeks, or more to develop their solutions (cf. [10]).

6 Model Limitations

In this section, we outline limitations and open problems of our proposed model.

1. Session scheduling

Students may share their pre-assigned meeting codes, making it possible to attend each other's rooms via separate devices.

2. Session setup

- In the setup where students share examination rooms, students may use multiple screens and monitor other students on a second screen without being noticed by the examiner.
- Videoconferencing software is typically resource intensive (CPU, memory, and network), which limits the number of rooms which any given examiner may join.
- In the setup where multiple students share an examination room, each of their individual screens and camera streams may be too small to view simultaneously and require multiplexing.
- In the setup where multiple students share an examination room, it may be possible for one student to view the contents displayed on another student's screen and retype them in their own work.

3. Student identification

- It is arguably easier to fake official documents when they cannot be examined physically but are rather transmitted (often with poor quality) via a webcam: it becomes difficult to distinguish a real identification document from a fake one. Thus, this check becomes a weak point.

4. Screen monitoring

- In case the student is running the exam in a guest OS inside a host OS, only the contents of the guest OS will be visible. This allows the student to perform all kinds of additional activities on the host OS. It should be noted that this risk is partially mitigated in the case when a mobile camera is used to monitor the student and their physical screen and how they interaction with the computer.
- Additional software may be running in the background, not visible on the screen of the student. Such software could allow other people to log in remotely to the student's computer and help them solve the exam. It may also record the contents of the screen and transmit them to a third party.

5. Auditory and visual monitoring

- A single camera is unable to capture the entirety of the student's surroundings. Even worse, in the case of an embedded laptop camera, only the student's face and some of their surrounding background are shown, which is arguably unsatisfactory as means for visual monitoring. The latter problem is mitigated by the use of a mobile camera, as described in the previous section.
- It may be argued that a request to monitor and record the student's private space from which they are working from may be viewed as a privacy violation. This is mitigated by the fact that the student can choose the location from which they decide to take the exam, which part of their surroundings is visible, as well as having no other students, or a limited number of other students being able to view their video stream, in addition to the examiner.
- One problem, which remains unresolved, is the loss of Internet connectivity. As students use regular service plans at home, normally they cannot be expected to have backup connections, or high levels of availability, which a larger enterprise can afford. Thus, it is possible that a student will lose connectivity during the exam and thus to drop out of a meeting for a significant period (say half an hour or more) and later to reconnect. This is undistinguishable from a case, where a student intentionally breaks their connection for some time. During that time, they will not be sharing their screen and camera with the examiner and this allows them to receive help from a third party. Unfortunately, we have not identified any good solutions to this problem. Assuming that by default our students connect to Internet via a cable, we have advised the students to also be ready to quickly switch to a secondary connection provided by their mobile operators in case of a connection loss. A careful balance needs to be made here. On one hand, if such occurrences are completely ignored, this opens the door to cheating. If, on the other hand, every connection drop results in

the student being failed at the exam, this may unfairly penalize students for factors that may be out of their control (such as the state of the network of their service provider).

As a possible compromise, we propose the following policy: if the connection drop lasts only a few seconds, it can be ignored. Otherwise, the student is considered to have failed the exam and is assigned no grade. To compensate, another exam may be scheduled on a later date, which will give the student second chance. Another solution is to note such events and to conduct an additional interview at the end of the course with all students who have had cases of a dropped connection.

- Similar problems arise from hardware and software failures, whether honest or simulated intentionally. The same arguments apply as above.

6. Session recording

- When the recording is independently performed by the videoconferencing software, typically the examiner has little or no control over what is being recorded. This may pose a problem in multiple screen-sharing sessions, where not all screens and video streams may be visible on the recording at the same time.

7. Solution submission

- It is technically possible for the student to submit stealthily another file, if it has been remotely copied to their computer in place of the file they were editing, especially if the solution is essentially the same but with bugs fixed which is unlikely to arouse suspicion.

8. Plagiarism detection

- This measure is not effective in cases when the solution is not provided by another student taking the exam, but by a person, who provides a unique solution. (For example, a friend, a relative, a hired person, etc.). Obviously, in such cases there is no way to get a match with another solution.

7 Conclusion

The results described in the article reflect the experience of more than 15 teaching and examination teams led by the authors with more than 1000 students over the period of April 2020 – April 2021.

The model proved to be successful in practice, with essentially no students being failed due to technical problems or cheating attempts. The opportunity provided to the students to attempt the exam more than once may have been crucial for reducing the level of stress caused by the unusual circumstances. We should note that the fact that the exams were held in the Bachelor programs in the area of Computer Science. It is implying a degree of technical savviness, combined with the fact that the nature of the subjects in question allowed examinations to

be carried entirely on a computer, had probably contributed to the relatively low number of technical difficulties that we had experienced throughout the examinations conducted according to our model.

We observed a distribution of grades similar to what we observed in previous years, leading us to conclude that there was likely no significant positive or negative bias due to the fully online nature of the examination (and education in general).

We conclude that our proposed model may successfully serve as a replacement of an in-person examination. As potential future work, we plan to explore alternatives for addressing some of the deficiencies of the model identified in this paper. Furthermore, we would aim to examine its applicability, possibly via appropriate extension, to other types of computer science examinations, where the problems expect students to produce definitions, process descriptions, requirements, or diagrams (e.g. [11]) instead of programming code, as well as to other subject areas in general.

8 Acknowledgements

The authors gratefully acknowledge financial support by Sofia University "St. Kliment Ohridski" grant 80-10-173/05.04.2021.

References

1. Moodle.org Homepage, https://moodle.org, last accessed 2021/04/11.
2. Kaloyanova K.: An Educational Environment for Studying Traditional and Big Data Approaches, In: Proceedings of INTED2018 Conference, pp: 4270–4274. IATED, Valencia, Spain, (2018).
3. Armyanov, P., Semerdzhiev A., Georgiev K., Trifonov T.: The Effects Of Incremental Grading And Optional Homeworks On Student Motivation, In: Proceedings of INTED2018 Conference, pp: 618–625. IATED, Valencia, Spain, (2018).
4. Safe Exam Browser, https://safeexambrowser.org/, last accessed 2021/04/11.
5. Google Meet Homepage, https://apps.google.com/meet/, last accessed 2021/04/11.
6. Google Meet for Education, https://edu.google.com/products/meet/, last accessed 2021/04/11.
7. Prechelt L., Malpohl G., Philippsen M.: JPlag: Finding plagiarisms among a set of programs. Univ., Fak. für Informatik (2000).
8. Schleimer S., Wilkerson D. S., Aiken A.: Winnowing: local algorithms for document fingerprinting. In: Proceedings of the 2003 ACM SIGMOD international conference on Management of data, pp. 76–85. ACM, New York (2003)
9. Novak M., Mike J., Dragutin K.: Source-code Similarity Detection and Detection Tools Used in Academia: A Systematic Review. ACM TRANSACTIONS ON COMPUTING EDUCATION, Volume: 19, Issue: 3, Article Number: 27, DOI: 10.1145/3313290, Published: JUN 2019
10. Semerdzhiev A., Trifonov T.: Practical aspects of plagiarism detection in computer science e-learning. In: ICERI2013 Proceedings. IATED, Valencia, Spain (2013).
11. Kaloyanova K, Orozova D.: How to Apply ISO/IEC 27001 to the Education in Information Security Area, Computer and Communications Engineering 13(2), 81–84 (2019).