E-exams versus paper exams: A comparative analysis of cheating-related security threats and countermeasures

Guttorm Sindre, Aparna Vegendla
Department of Computer and Information Science (IDI), NTNU

Abstract

E-exams can have a lot of advantages over traditional paper-based exams, and if using a BYOD approach (Bring Your Own Device) they can also scale to large classes and peak exam days. At the same time, BYOD adds extra security challenges by using student-controlled equipment. To be viable, BYOD e-exams need not have perfect security, only about the same level of security as paper-based exams have. This article uses attack-defense trees to provide an analysis comparing the threats and countermeasures against cheating at controlled exams with paper-based exams versus BYOD e-exams. The conclusion is that neither has a clear advantage from a security perspective.

1. Introduction

A number of advantages have been reported for computer-based assessments over traditional paper-based examinations [1-7], both in terms of computer support for question development, reduced cost of test distribution and administration, reduced cost of distributing answers to graders, and possible automated support for grading. Additionally, new types of test items (e.g., based on audio, video, 3D engineering models, industrial tools, and interaction) can be enabled, thus giving a test with much higher validity vs. professional work practice.

At the same time, there has been reluctance towards introducing e-exams in many universities. This is for instance the case with our own university (NTNU) where most proctored school exams are still traditional paper exams, except a just beginning practice of having e-exams in a limited number of courses with a limited number of students. Two main concerns towards replacing paper-based exams with e-exams are scalability and security. Scalability is a major challenge especially if tests are to be performed on university equipment. With a Bring-Your-Own-Device (BYOD) approach, where students use their own portable PCs, scalability will improve, but at the cost of added security challenges since the client device can more easily have been tampered with before the exam to facilitate cheating. However, paper-based exams do not have perfect security either [8-9]. Hence, if e-exams have advantages in other respects they need not have better security than traditional paper-based exams, only a similar level of security. So, it is interesting to compare BYOD e-exams and paper-based exams with respect to cheating-related security. In this paper, we will use Attack-Defense Trees (ADTrees) [10] in this analysis, these are an extension of traditional attack trees [11] where there are defense nodes in addition to attack nodes.

For reasons of space and focus, we limit the scope of our paper in several ways. We do not discuss other aspects than security in any detail, though in another paper we have looked more at didactic issues and process improvement potential of e-exams [12]. The focus on this paper is on the cheating challenge, so we only consider cheating-related security threats to exams. For instance, this means that denial of service attacks against exam servers will not be discussed in this paper. A successful DoS thwarting an entire exam would be very serious and necessary to protect against, but it can hardly be categorized as cheating since nobody achieves an unfair grade advantage. Also, we limit our discussion to cheating during the exam, not before or after. The rationale for this choice is that cheating before or after the exam is not so dependent on the choice of
paper or PC as the medium for the student's answer. Moreover, we focus on written school exams, not other types of assessment tasks. Some types of cheating are even easier for uncontrolled home exams (e.g., impersonation, undue assistance), but using uncontrolled home exams is an implicit choice not to mitigate such cheating threats, and therefore less interesting to analyze in this context.

With a quick intuitive take, BYOD e-exams may seem obviously less secure than paper exams. In a consultancy report in connection with the ongoing project to digitize the exam process at the NTNU, it is said that it is relatively easy to enforce strict rules to prevent cheating with traditional paper exams, while it is much more difficult for digital exams [13]. Similar views can be found in international academic literature, most precisely stated by Dawson: “The BYOD eExam is by definition less secure than both pen-and-paper examinations, and examinations held in a computer laboratory, as it has all the vulnerabilities of both environments, as well as some of its own.” [14] (p.7).

In our opinion, this claim is exaggerated, although Dawson is obviously right that e-exams may have several serious cheating threats that paper exams do not have. For instance, the following threats can easily be envisioned related to the PC:

- Electronic communication between candidates, or with assisting outsiders.
- Copy-paste plagiarism of allowed or non-allowed sources.
- Peeking at neighbor answers might be easier due to the upright angle of screens.
- The PC can contain materials or tools not allowed for the exam.
- Bigger amounts of information can be crammed into smaller objects (e.g., memory sticks rather than paper), yielding more effective cheating by object passing, either directly between candidates in the exam room, or by using the restroom as a mailbox.

It is also easy to agree with Dawson that many of these threats are worse for BYOD e-exams than for e-exams using university equipment, because students could more easily have tampered with their own PC (e.g., installing materials or tools not allowed, or rigging the PC to circumvent security functions of the exam system). However, what seems to be ignored in the statement that BYOD e-exams are "by definition" less secure than paper exams, is that e-exams – in addition to introducing new threats – also enable many countermeasures against cheating. Some of these countermeasures are effective not only against the threats particular to BYOD e-exams, but also against a wide variety of traditional cheating threats. This complicates the picture and means that it is not at all obvious that BYOD e-exams will generally be less secure than paper exams. Rather, this will depend on the exact implementation of the paper exam, and of the e-exam.

Our research questions for this paper are as follows:

- RQ1: What cheating threats exist for the typical school exams of Norwegian Universities like the NTNU?
- RQ2: What are the main differences in possible threats and countermeasures for paper exams and e-exams?
- RQ3: What requirements are important for secure BYOD e-exams?

The rest of the paper is structured as follows: Section 2 gives a quick introduction to some countermeasures that are better enabled with e-exams than with paper exams, to justify early on our disagreement with arguments that BYOD e-exams are necessarily less secure. Section 3 then gives a more systematic discussion of cheating threats and countermeasures, comparing paper exams and BYOD e-exams by means of ADTrees. Section 3 then makes a more systematic comparison of threats and countermeasures, to see which risks increase by e-exams and which decrease. Section 4 discusses related work, whereupon section 5 concludes the paper with some ideas for further work.
2. Improved countermeasures in e-exams

A key countermeasure in school exams is the use of proctors to oversee the candidates during the exam and catch candidates who cheat. This is the main defense against cheating in paper exams, and could be used similarly for e-exams. However, research indicates that students may be able to cheat in spite of the presence of proctors [15]. An important insight in security research is defense in depth. For exams this would motivate other barriers towards cheating in addition to proctors, and some of these are much easier to implement with e-exams than with paper exams, as will be argued in the following paragraphs:

**Mixed seating.** Instead of having students of the same course seated row by row in the same exam room, mixed seating of many different courses could effectively mitigate cheating by close range collaboration (whispering, peeking at neighbor's answers, passing answer sheets or other information objects). For paper exams, large scale mixing is hard due to the increased workload of sorting question sets into room piles before the exam day, and complicated distribution of questions on the day. Mixing would also give teachers a hard time if they need to come to the exam room to clarify issues with the exam questions. For e-exams, distribution of questions and collection of answers can be fully automated. Clarifications to questions could be done online, which not only makes this task easier for the teachers, but also improves fairness as all candidates of an exam could get the same information at the same time.

**Non-uniform questions.** Identical question sets to all examinees makes collaborative cheating much easier, since it suffices to communicate the answers. For instance, the solution to a 100 item multiple choice test can be communicated with 100 letters A/B/C/D, 50 HEX symbols, or even fewer signs using various compression techniques. This is easily within reach of what can be communicated by SMS, code signals, or simply written on a piece of paper to be dropped in a previously agreed WC trash bin to be picked up by somebody else. Randomizing the order of questions makes such cheating much harder for multiple choice and short answer questions, since it increases the cheaters' communication burden when question information must also be included. Such randomization is easy for e-exams, while much harder for paper exams due to more cumbersome printing and copying of question sets.

**Moving calculators and books into the exam system.** Calculators and allowed books are well known vulnerabilities for cheaters, who might hide forbidden information in calculators or books, or even transfer information if allowed to share resources. With e-exams, the calculator could be an app provided by the exam system, obliterating brought calculator devices. Allowed written resources could be provided digitally through the exam system, this obliterating the need to bring books. For paper exams, allowed written materials can of course be printed as an attachment to the question set, but this only works in cases where it is just a couple of pages (e.g., some few formulas), otherwise it will be way to expensive in terms of copying costs.

**Strict question/answer sequence.** If you want to cheat by getting assistance from one or more outsiders, it is often preferable to use as few communications acts as possible, ideally just two. You export the questions just after the start of the exam (e.g. photographing with a smart phone and send as MMS, or smuggle questions to agreed WC trash bin for pick-up by the accomplice). Then you get answers back later (again various options for how to do this). One way to mitigate such cheating is to reveal questions in strict sequence (i.e., Q2 is only shown to the candidate after a no-return response has been submitted to Q1, etc.). Then, cheater and accomplice would need much more frequent communication, which would be riskier. Whether to use this mitigation or not, could however depend also on other factors. For some types of tests,
the teacher might want the students to be able to revisit previous questions and improve their answers for the duration of the exam.

Automated plagiarism checking. With digital answers, tools for plagiarism checking can be used effectively, not just for direct copy paste, but gradually also for various rephrasing tricks. This kind of cheating then becomes much more risky than it were for paper exams.

Biometric authentication. Impersonation - i.e., having somebody else sit the exam for you - is a rare cheating threat, but potentially the most effective of all if uncaught, since even an F candidate can get a perfect A if the impostor has strong subject knowledge. The current approach with student ID cards is insecure in case a candidate knows a willing impostor with a quite similar face. Also, there are services on the internet for buying custom fake ID cards. Biometrics is assumed to give far better security [16]. Of course, this could be employed both for paper and e-exams, but e-exams have an advantage that infrastructure for the authentication is then anyway in place, e.g., using recognition of face, voice, and keystroke dynamics via the same PC that is used for answering the questions. For a paper exam, equipment for such authentication would instead have to be provided by the university and e.g. carried around by the proctors, giving extra cost.

Above we have mentioned six important countermeasures against cheating. All of them are in theory possible also for paper exams, but will be more costly or cumbersome than for e-exams. This should serve as sufficient illustration of our point that BYOD e-exams are not necessarily less secure than paper exams. This should also justify that a more detailed comparative analysis of cheating threats and countermeasures of e-exams and paper exams might be of interest. Such a comparison will be provided in the next section.

3. Detailed comparison of cheating threats and defenses

Cheating can be defined as behavior which is against the regulations of the university or of the particular exam, and which may give some candidates an unfair advantage over others. A detailed treatment of cheating in legal terms is beyond this paper (and these authors), the reader can consult [17] for a discussion related to Norwegian law.

From how-to pages on the web it can be inferred that there is a wide variety of cheating methods, even in invigilated school exams¹, all the way from old-fashioned crib-notes and peeking at the answers of others to high-tech cheating with smart phones and miniature spy equipment. Hetherington & Feldman [18] present a taxonomy of cheating with four categories: individualistic-opportunistic, individualistic-planned, social-active, and social-passive. Björklund & Wenestam list 23 ways of cheating in the appendix of their article [19]. In our paper, we will use a list with somewhat broader categories still thought to cover those of the referenced works. New threats specifically occurring with e-exams are in italics in the list below:

1. Impersonation: Having your exam answered by somebody else.
2. Assistance / collaboration: Candidates get assistance from other candidates, employees, or outsiders, or collaborate in a way not allowed for the exam.
3. Plagiarism: Presenting somebody else's words or ideas as one's own, i.e., without proper referencing and quotation marking.

4. **Using aids not allowed for the exam**: Most exams have restrictions on usage of materials (e.g., textbooks) and tools (e.g., types of calculators).

5. **Timing violation**: The candidate starts to work on the exam before allowed, or continues to work after the exam inspector has declared that time is out.

6. **Lying to proctors** to achieve some favorable outcome. One example of a favorable outcome could be to get extra time on the exam or leniency in grading, due to a claimed (but not real) problem with the exam. Another example could be to have an exam attempt cancelled rather than failed, for instance by faking disease during the examination.

7. **Smuggling out the exam questions after the exam**. Some universities consider this a serious offense, typically because the same questions may be reused in subsequent tests. In Norway, this is seldom the case. At the NTNU previous exams are normally publicly available documents and students are allowed to keep the questions when the exam time is out.

Discussing all these threats in detail will be too much for this one paper. Hence, we decide to drop the least important ones. #7 is not so relevant in Norway. #6 is believed to be rare, and the ability to fake disease is not affected by the choice of paper or e-exam. #5, although relevant, will seldom give a huge advantage in grade, e.g., getting a couple of minutes extra is not likely to help much if you were not able to answer questions during the 3 hours that the exam really lasted. Finally, plagiarism (#3) tends to be more relevant for home exams and term papers than for school exams. Thus, our further analysis here will focus on the three threats of impersonation, assistance / collaboration, and using aids not allowed for the exam, to be analyzed in the next subsections.

### 3.1 Impersonation

An attack-defense tree for impersonation is shown in Figure 1. The attack nodes (red ovals) indicate what a cheater tries to achieve. In this particular diagram, all decompositions of attacks into sub-attacks are OR-relationships, as no arc is connecting the lines. Laptop and paper icons are not part of the original ADTree notation but are used for illustration here. Having such an icon placed next to a green rectangular defense node indicates a potential advantage for that type of exam, i.e., the defense is more feasible. Having it next to a red node indicates a disadvantage: that type of exam is more vulnerable to the particular attack. Hence, it indicates two main impersonation attacks:

Since the rightmost branch ("Label swapping") is the simplest, we discuss this first. This would entail that two students collaborate, and each identify correctly as themselves. However, upon delivery of the answers, candidate X instead labels his answer with Y's candidate number, and vice versa. Mitigations would be either than the proctor checks that the correct number has been written, or that even the proctor writes the number (the candidate not knowing it in advance). For an e-exam, explicit labeling might not at all be needed, as this could be done automatically and internally in the system based on the authenticated identity of each candidate.

To prevent spoofing one must verify the candidate's identity. The traditional approach is to require a picture ID of the candidate, but this is vulnerable both to look-alikes and fake ID cards (left sub-tree). With a BYOD e-exam it would be possible to authenticate the candidate by username + password instead. However, username + password would be much less secure than even the picture ID, since the candidate could simply give his login credentials to the impostor before the exam. Hence, this option is crossed out (this cross not a part of the original ADTree notation, but used for
illustration purposes here). Biometrics seems to be the better choice, and as argued earlier e-exams can enable this more cheaply. However, like passwords, biometrics can also be vulnerable to replay attacks. With proctor-provided equipment, the only feasible attack would be an external replay (e.g., wearing a fake fingerprint, pretending to speak into a device for voice-recognition while really playing a recording or live streaming of the real candidate from a small hidden device, holding a picture of the real candidate's face in front of the camera). From these examples, it seems that face recognition would be the most secure of these three options. It is easy to produce fake fingerprints, but very hard to produce masks to fool face recognition, and it is harder to hold up a picture unnoticed by the proctors than to play audio from a hidden device.

Using the BYOD laptop, which the candidate and impostor might have rigged for the purpose beforehand, an additional attack of censor bypass might be possible (e.g., the laptop pretends to be sending the server live video of the examinee from its camera, while it really streams recorded video from a file). Thus any advantage of cheaper biometrics for BYOD e-exams might be partially dissipated by the additional attack available. However, both types of replay attacks can be mitigated by the same means, namely adding some control information not known to the examinees beforehand. Hence, if using voice recognition, you would not only demand candidates to state their names (which could easily be pre-recorded) but also to add a phrase provided by the proctors just at authentication time. If using face recognition, you might demand recognition of the background of the exam room, or of a proctor-provided visual cue, in addition to the examinee's face. Hence, the threat of censor bypass does not introduce the need for a lot of new defenses. All in all, therefore, e-exams seems to have the potential to be more secure than paper exams versus impersonation because they can easily mitigate the Label swapping threat, and may offer biometrics at lower cost than what is the case for paper exams.

3.2 Assistance / collaboration, and Unallowed aids

While impersonation might be rare, collaboration and usage of forbidden materials are much more common cheating practices. As argued in Section 2, e-exams can offer a
lot of countermeasures which are practically infeasible for paper exams, and some of these countermeasures are effective against several different types of cheating, both collaborative (getting assistance from other examinees or outsiders) and individual (e.g., using unallowed materials during the exam). An ADTree for Assistance / Collaboration is shown in Figure 2, and an ADTree for Unallowed Aids is shown in Figure 3. As can be seen from these figures, the laptop is associated with a number of countermeasures already mentioned, like Mixed seating, Non-uniform questions, and enforcing a Strict Q/A sequence. These all contribute to mitigating attacks related to traditional in-room communication between candidates, as well as peeking at neighbor answers (which might be done even if the other does not knowingly collaborate). Non-uniform questions also mitigates collaboration via the toilet, since answers hidden there by one candidate might not be relevant to an accomplice retrieving them. A strict Q/A sequence mitigates both collaborative and individual cheating (e.g. hidden resources) in the toilet, as a candidate would need to make suspiciously many toilet visits, whereas with a paper exam one visit to the restroom could be used to check many questions.

Looking specifically at Figure 3, we have already touched upon peeking (leftmost subtree) and cheating in WC (middle). In the exam room, cheating can otherwise be done with concealed aids (e.g., small, hidden cheat note) or with aids that can safely be put on the desk. For concealed aids, it is hard to see any advantage for either type of exam. However, there might be a difference for desk aids. In a paper exam, a cheat sheet which is or looks sufficiently similar to an official drafting sheet for exam usage, can safely be put on the desk as long as the cheater waits some necessary minutes after the start of the exam time, so that the contents is something he could plausibly have written after the exam started. Then, the only really risky moment for the cheater is the second he spends pulling the sheet from a hidden location (e.g., under T-shirt) and placing it on the desk. Thereafter it can safely reside on the desk and help him throughout the entire exam. Having a paperless exam, however, would suddenly make the possession of such a sheet risky all way through. This could be possible with BYOD e-exams, though not all, as the candidates may need to use paper for drafting. For instance, in a math exam with multiple choice questions, candidates would likely need
to make the calculations to know which answer alternative would be the correct one. Hence, the paperless exam mitigation would only be reasonable in courses where no drafting would be needed, or where drafting could best be done on the PC anyway.

In addition to the possible advantage of a paperless exam that cheat sheets are no longer plausible items to have on the desk, it also means that a number of other utensils like pencils, erasers, rulers etc. become obsolete, and there are known cheating methods related to all of these. Doing away with calculators and brought books opens up a further advantage, both versus individual cheating (as these resources may also contain other hidden material) and collaborative cheating (if a proctor allows two candidates to share such a resource, for instance because one had forgotten his book or suffered a calculator malfunction). Another potential advantage of e-exams is that they limit proctor tasks. In paper exams, proctors are responsible for supplying candidates with more answer sheets, collecting answers when candidates deliver, and requesting the presence of the teacher if candidates suspect errors in the question set. With e-exams the latter task can go online, and the two former disappear, hence proctors can concentrate better on their primary task of detecting cheating.

The Fake/Corrupt employee threat (Fig 2) is assumed to be rare, though one cannot totally exclude collusion between employees and candidates for reasons such as bribery, blackmail, or relationships (family, love, cults…). The Strict Q/A sequence countermeasure does not prevent a fake employee (e.g., posing as a teacher) or similarly bribed one to come to the candidate's desk, but it makes the attack less effective. If the candidate can only get help with the one question he is currently at, the accomplice might need to make many visits to the candidate's desk for the help to be substantial in terms of grade improvement. This would make the operation much more suspicious.

Indeed, strict Q/A sequence would also mitigate some threats of communication via laptop or small wireless devices. Sending questions to an accomplice early on (email with question file, MMS with photo of questions,...) and getting answers back later would be hard, instead one would be left with the need to communicate more frequently which would likely be riskier. To prevent against continuous communication between
candidates, or with outsiders (e.g., using a background Skype call with shared screen as exemplified by Dawson [14], or using a wireless mini camera to export questions, a wireless earplug to import answers, both connected to a small GSM box to facilitate communication with a person outside the exam room), one must either rely on prevention or detection. For the laptop, prevention approaches would typically include forcing the candidates to boot using a proctor-provided USB memory stick, and/or using a lockdown browser, so that candidates are prevented from opening files or programs not allowed during the exam. Detection approaches might include monitoring of the screens of the laptop (e.g., by taking screen shots of student laptops at regular intervals, as is done at the University of Southern Denmark (SDU)\(^2\), and by installing cameras in the exam room), as well as the monitoring of laptop audio (to prevent usage of the laptop for e.g. background Skype conversations), keystrokes (e.g., to discover if a large chunk of text suddenly finds its way into the answer by other means than being typed by the candidate) and running programs. Also, one could monitor the network traffic related to each PC, as for instance a background skype call or sending questions to an outsider would have a quite different communication profile from the normal question/answer work through the e-exam tool.

Of course, there may be legal implications of electronic surveillance of the students during the exam, and there are several questions concerning this that are unclear in Norwegian law [21]. Hence, although a certain kind of surveillance is used at the SDU or other places, this does not guarantee that the same type of surveillance is possible in Norway. If using their own laptops for the exam, students of course also have a lot of personal information on these devices, possibly also of a sensitive nature. So it could expected that, e.g., the exam system taking a copy of all files on every student's PC, would not be allowed. From the web page of the University of Southern Denmark\(^2\) it seems that the system only inspects active files and programs and communication in/out from the PC, but not passive files on the computer. A legal discussion whether this would be legal in Norway is beyond the scope of this paper, but will likely be clarified if a Norwegian university takes a similar approach. The legal argument in favor of some surveillance would be that, unlike traditional cheating, electronic activity inside the laptops cannot possibly be seen by proctors, so there needs to be some other kind of mitigation in place to avoid easy cheating.

As is suggested by the attack node "Small device" second to the right in Figure 2, the laptop is not the only possible means for electronic communication among candidates or with outsiders. Cell phones and other small devices can also be used. To mitigate against this, one could try to jam such communications if this is legal (prevention), or to scan for them (detection). Although a deep comparative analysis of the PC threat versus the small devices threat is beyond the scope of this paper, it seems that using the laptop for cheating might in many ways be riskier than using small devices. There are more effective monitoring approaches available for the laptop, especially if collaborative cheating is attempted through the established network. With small devices it is more difficult to discover, and even if some bluetooth, radio, or other signals are discovered, it is hard to know exactly what candidate it came from.

4. Related work

Sheard et al. [22] presents the survey on cheating and plagiarism with undergraduate IT students in two universities. The survey was conducted by a questionnaire based on 18 scenarios. The students were asked to rate their perception on

\(^2\) https://em.sdu.dk/
scenarios on a 5-point Likert scale. The survey was performed on cheating, but without any comparison of paper vs. e-exams. Hillier [23] has made a questionnaire survey comparing student perceptions of e-exams versus paper exams. The study is not particularly about security, but touches upon security, too. The students on average thought that e-exams would be less secure than paper exams, but the difference was not massive. King et al. [24] made a survey with 121 business students, where students believed it was easier to cheat with online exams.

Sclater and Howie [7] present a number of requirements to e-exam systems, a couple of these are security requirements. Other works have looked at specific protection mechanisms such as cryptographic schemes [25] and security protocols [26].

Clariana and Wallace [27] compared paper based versus computer based assessments, but not particularly security. Instead they focused on student performance, and concluded that higher attaining students benefit more from computer-based assessments compared to paper-based ones. Another comparison by Jamil et al. [28] focuses on teachers’ perceptions, concluded that attitude among their informants was quite positive towards computer-based examinations, though in some cases, teachers preferred paper as well.

Except for the quite brief and crude statement by Dawson that BYOD e-exams are less secure than paper exams [14], and some surveys and general investigations touching upon security issues, this paper is to our knowledge the first more detailed comparison of cheating-related security and countermeasures of paper vs. e-exams.

5. Discussion and conclusion

If BYOD e-exams fail to utilize the several new countermeasures that become feasible in a paper-less process, one could agree with Dawson that BYOD e-exams would by definition be less secure than paper-based exams. Even if using lock-down browsers like Safe Exam Browser\(^3\), as well as monitoring the screens, keyboards, camera, audio, and network traffic of the laptops during the exam, one must imagine that some students may be able to perform cheats that go under the radar – for instance by having installed software on their laptops to conceal illegal activities as legal ones.

On the other hand, the case for e-exams is that they offer a wide range of countermeasures that mitigate a number of cheats, such as mixed seating, non-uniform questions, strict Q/A sequence, and reducing the need for brought items. Hence, a number of known cheating techniques are suddenly much less effective. Moreover, for some types laptop-enabled cheating, such as electronic communication between candidates or with outsiders, the laptop might not be the device of choice for the potential cheater. It is much easier for the exam organizers to monitor a laptop which they know is there, and which is hooked up with their network, than to monitor the usage of small devices which they do not know about. Also, if detecting suspicious network traffic from a laptop, one can quickly determine which candidate it is associated with, but this might be much more difficult if the candidate is using some type of wireless communication from a miniature device. Hence, even for the new threats that it brings, the laptop might not be the weakest link in the chain, as spy equipment like wireless earplugs and micro cameras are becoming ever smaller and cheaper, and partly advertised specifically as exam cheating equipment.

To avoid becoming less secure than paper-based exams, it is however important that BYOD e-exams utilize the countermeasures it has as its disposal. Hence, exam organizers should utilize mixed seating whenever feasible. If teachers are required to

\(^3\) http://safeexambrowser.org/news_en.html
provide clarifications to question on the exam day, the exam system must support requests and clarifications online. Otherwise, mixed seating is difficult. Online clarifications also improve fairness, as all get the same information at the same time. Non-uniform questions should be utilized whenever there is otherwise a big cheating threat in answers that can be quickly communicated or seen by peeking at neighbors (e.g., multiple choice or short answers). Calculators, dictionaries and other allowed books should as much as possible be provided as digital resources in the exam system rather than as traditional brought objects, as this reduces some well-known cheating vulnerabilities. A strict Q/A sequence might feel inappropriate in some types of exams, but if it is used, it certainly makes several types of cheating much harder, especially related to communication among candidates or with outsiders (via electronic equipment, or using the restroom as a mailbox). Hence, digital exam tools should have a setting for the teacher to decide whether questions must be answered in strict sequence or not.

As a final conclusion, this paper of course has a number of limitations. It is far from a complete and systematic treatment of every possible cheating threat, and there is little technical detail about particular threats relating to student laptops. Yet, it has pointed out some possible countermeasures that e-exams have against cheating which are infeasible for paper exams. While this certainly does not show that BYOD e-exams are more secure than paper exams, but at least demonstrates that they need not be less secure, as the level of security will depend on the actual implementation of each exam type, what countermeasures are in place, the skills of the proctors, and the types of questions asked on the exam. Further work is needed to arrive at precise security requirements for e-exam systems, and this would have to include both technical requirements for the e-exam tool and infrastructure, and organizational requirements concerning training and awareness of proctors to handle this new mode of examination.

References