

Fraud-Resistant Computerised Examinations

Version 1.2 of 20 November 2015


Kees Goossens and Martijn Koedam

ES Reports

ISSN 1574-9517

ESR-2015-03
20 November 2015

Eindhoven University of Technology
Department of Electrical Engineering
Electronic Systems



© 2015 Technische Universiteit Eindhoven, Electronic Systems.
All rights reserved.

<http://www.es.ele.tue.nl/esreports>
esreports@es.ele.tue.nl

Eindhoven University of Technology
Department of Electrical Engineering
Electronic Systems
PO Box 513
NL-5600 MB Eindhoven
The Netherlands

Fraud-Resistant Computerised Examinations

Kees Goossens and Martijn Koedam

Version 1.2, dated November 20, 2015

1 Executive Summary

The immediate and focussed problem that is addressed in this document is:

How can a student use a computer to enter answers to an examination in a way that is not more susceptible to fraud than a paper-based examination?

The computer may be brought by the student (bring your own device, BYOD) or be supplied by the university. Whether the exam is graded automatically after it has been entered, or not, is an orthogonal concern, and we return to it later. We assume that exam answers are entered on an exam website, in particular (exam.)oncourse.tue.nl.

In Essence

Students should not be allowed the following:

1. Access to disallowed information, including communication with others.
2. Access to the examination outside the examination period.
3. Access to the examination outside the examination location.
4. Share access to the examination attempt with another person.

We implement these restrictions with:

1. Controlled access to information — to solve problem 1.
 - (a) Block all network access on computer, except to the exam website.
 - (b) Block all access to the file system.
 - (c) Exam website with only exams, and not allowing any communication.
2. Controlled access to the exam attempt — to solve problems 2-4.
Implemented with a *physical token* that is available only in the exam location for the duration of the exam.

Our Solution: The Examiner

Our solution works for both university-managed computers and bring your own device (BYOD) and is comprised of:

1. A dedicated *exam.oncourse.tue.nl* website, with restrictive (quiz) settings.

2. Our *Examinator dongle* (USB stick) per student. Experience shows it works for 90+ % of students. Scales to hundreds of students. A computer server is used for configuration per exam, and authentication per student. Cost of a few euros per dongle.
3. For all remaining students, no good solution is available, in the sense that all options are laborious and/or easily allow fraud. We have used traditional paper-based exams (graded manually or automatically), personal codes for use with Oncourse, and a common (un)shareable secrets (i.e. passwords) for use with Oncourse.

Our solution reduces work when: a) the number of students taking the exam is large enough, and b) the percentage of students for which the Examinator dongle works is high enough.

The Examinator can be used on both BYOD and university-supplied computers. It has been successfully used in 10 exams of first & third-year BSc and first-year MSc in both intermediate and formal exams with up to 350 or so students simultaneously.

Conclusions

We have developed a promising first solution to allow students to use their own computers to enter questions to exams, without (computer-related) risks of fraud.

Technically, some additional steps must still be taken, particularly regarding browser authentication, and the impact of the Examinator dongle use on the TUE infrastructure.

Non-technically, the Electronic Systems Group will further develop the Examinator for its own use. However, the most pertinent question is if the Examinator deployment should be broader, i.e. TUE wide. If yes, then who will develop, maintain, and deploy? The cost-performance trade-offs of various deployment options are discussed in detail in Section 7.

Version history

1.1 First version for public release.

1.2 Added evaluation of booting over network instead of USB stick (pages 9 and 15), and e-Exam (transformingexams.com) on page 12.

Contents

1	Executive Summary	1
2	Background and Problem Statement	4
2.1	Choice of Oncourse (Moodle)	4
2.2	Problem Statement	4
2.3	Structure of this Document	5
3	Threat model	6
3.1	Example Threat Scenarios	6
4	Requirements	7
5	General Solution Approaches	8
5.1	Access to Information and Examination	8
5.2	Impersonation	9
5.3	Collaboration	9
5.4	Overview	10
6	The Examiner	13
6.1	Operation	13
6.2	Ideal Scenario: Formal Exam	15
6.3	Ideal Scenario: Intermediate Exam	16
6.4	Scenario: Students with Time Extension	17
6.5	Scenario: Non-Dongle Students	17
6.6	General Considerations	17
7	Cost-Performance Analysis	18
7.1	Recommendations	20
8	Conclusions	21
9	Acknowledgements	21
A	Terminology	22
B	Oncourse Evaluation	22
C	Examiner Dongle	24
D	Experiments	25
E	Technical Recommendations	27
F	Student Instructions	30
G	Invigilator Instructions	31

2 Background and Problem Statement

Student numbers have increased by a factor four in recent years, without a commensurate increase in staff. (As an example, our first-year Computation course has 380 students, up from 239 in 2014 and 208 in 2013.) To manage the education load on its staff, the Electronic Systems Group in the Electrical Engineering Faculty decided to investigate automating aspects of teaching, simultaneously aiming to improve the quality of the education that we offer to our students. We consider the following components of teaching that could be automated:

1. Course communication
2. Lectures
3. Practica
4. Homework
5. Intermediate exams
6. Formal exams

The last bullets include both giving and scoring the homework or exam.

2.1 Choice of Oncourse (Moodle)

We choose to use Oncourse. Technically, Oncourse is a good unified education environment for bullets 1-4. Non-technically, Oncourse support by the Mathematics and Computer Science Faculty is excellent. Moreover, we use Oncourse because it is based on Moodle that is used world wide, and is open source with good documentation. Were Oncourse to be replaced by another system it would be easy to continue our substantial investment by running Oncourse or Moodle ourselves. See appendix B for a more detailed evaluation of Oncourse.

However, Oncourse does not work well as an examination environment (bullets 5-6). Basically, an Oncourse quiz can be created with the questions for the examination, and students access the quiz using the `oncourse.tue.nl` website. For this, however, students must have access to a (wireless) network. Without further measures, students can then use the Internet to access information and communicate with others during exams, which is not allowed. This situation is illustrated in Figure 1(a). A more detailed threat model is defined below, in Section 3.

2.2 Problem Statement

Given that we use Oncourse to give examinations, the problem that is addressed in this document is:

How can a student use a computer to enter answers to an examination in a way that is not more susceptible to fraud than a paper-based examination?

The computer may be brought by the student (bring your own device, BYOD) or be supplied by the university. Whether the exam is graded automatically after it has been entered, or not, is an orthogonal concern, and we return to

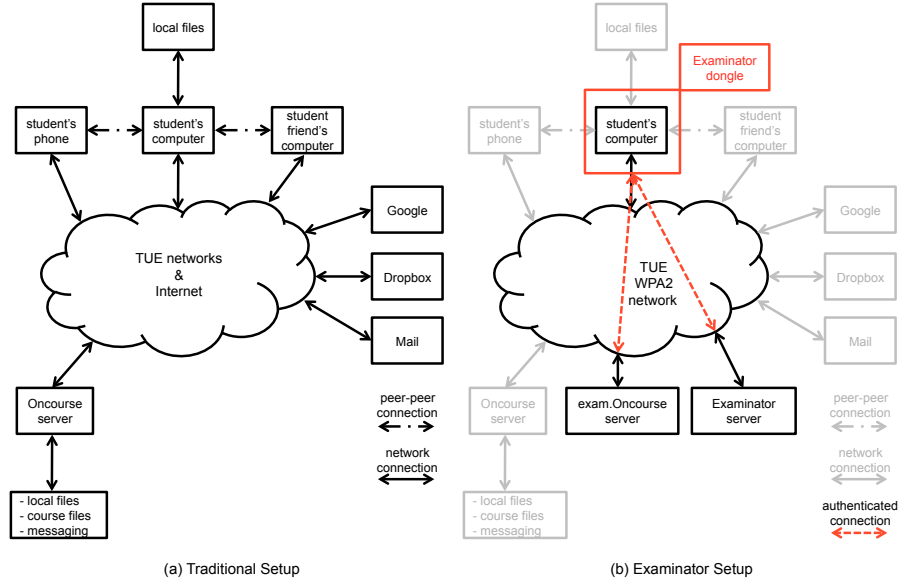


Figure 1: Computerised Exam Setup, (a) without and (b) with the Examiner.

it later. We assume that exam answers are entered on an exam website, in particular (exam.)oncourse.tue.nl.

2.3 Structure of this Document

Appendix A defines the terminology used in this document, in particular: examination versus attempt, and intermediate vs. formal exams. In Section 3 we first define our threat model: what is addressed and what not. This naturally results in the requirements that any solution to our stated problem should have in Section 4. We introduce a range of general approaches to solve our problem in Section 5. In Section 6 we then introduce the Examiner, and describe how it works and how it addresses the requirements. We also outline a number of fall-back methods that may be used when the Examiner cannot be used. Section 7 contains a cost-performance analysis of different solutions. We conclude in Section 8.

Appendix B contains a brief evaluation of Oncourse (Moodle), backing our choice for using it. Appendix D lists all experiments that we have performed with our Examiner dongle. Appendix C describes the Examiner dongle in more detail, and Appendix E contains a list of technical recommendations regarding Oncourse and the Examiner dongle. Appendices F and G contain instructions for students and invigilators that we have used for dongle-based exams.

3 Threat model

Students should not be allowed the following:

1. *Access to disallowed information.* Electronically accessible information includes: files on computer, files on media devices (dongles, etc.), files on Internet (Dropbox), Internet access (Google)*, and so on. We also include *communication with others*. In particular communication using the computer that is used: computer-phone & computer-computer communication using Bluetooth or WIFI, email, messaging/chatting/Skype, shared Dropboxes*, etc.
2. *Access to the examination outside the examination period.* Overall, easily solved. However, time extensions complicate this issue.
3. *Access to the examination outside the examination location.* For example, taking to exam without entering exam location*; access to exam after leaving the exam location, particularly when leaving early⁺.
4. *Share access to the examination attempt with another person.* For example, the attempt is done by someone other than the student, or multiple students collaborate on the same attempt.

We have observed 1 and 3 in our examinations, with those marked with a star (*) being most prevalent. While we have not observed + in our experiments, it is apparently widespread at the TUE.

Out of scope are traditional (non-computer) cheating methods such as writing on body, hidden pieces of paper, talking to other students, exchanging paper with other students, and so on.

Attacks to the examination infrastructure (modifying exams or submitted exam attempts, breaking into exam server, man-in-the-middle attacks, etc.) are only partially considered, and discussed later.

3.1 Example Threat Scenarios

General scenarios by which students can cheat:

1. Using disallowed information in files on computer during the exam.
2. Using disallowed information in Oncourse (e.g. lecture notes, uploaded files) during the exam.
3. Googling for information during the exam, or accessing other web sites, using Internet or peer-to-peer network.
4. Communicating with others during exam using Internet or peer-to-peer networks, using mail, instant messaging, shared Dropboxes, and so on.
5. Communicating with others during the exam using Oncourse messages and fora.
6. Giving others outside the exam location access to the attempt during the exam period (others can contribute to the same attempt as the student).
7. *Giving others at the exam location access to the attempt during the exam period* (others can contribute to the same attempt as the student).
8. Giving others outside the exam location access to the exam during the exam period (others can attempt the exam for the student).

9. *Giving others at the exam location access to the exam during the exam period* (others can then attempt the exam for the student).
 10. Not entering the exam location and doing the entire attempt outside the exam location (relevant for intermediate exams).
 11. Leaving the exam location early without starting the exam and doing the entire attempt outside the exam location (relevant for intermediate exams).
 12. Starting the attempt at the exam location, but leaving early and continuing the attempt outside the exam location (relevant for formal exams).
- Scenarios related to Examiner solution. Please consider these after reading Section 6.
1. Student fills in wrong dongle number (either non-existing, existing and not used in same exam, or existing and used in same exam).
 2. Students communicate and use same dongle number. This and the previous scenario may be combined with following scenarios.
 3. A dongle is lost.
 4. A dongle is not returned, but used in subsequent exam.
 5. A dongle is cloned (i.e. a copy with the hardware identifier of the original dongle, or a new hardware identifier).
 6. A dongle is reverse-engineered and modified (during exam, or after not being returned).
 7. The Examiner protocol is reverse-engineered and a dongle is impersonated on the Examiner or exam server.
- Scenarios related to fall-back setups:
1. Students communicate and use same personal code.
 2. Student fills in wrong personal code (either non-existing, existing and not used in same exam, or existing and used in same exam).

4 Requirements

The threats can be avoided with a solution meeting the following requirements:

1. Controlled access to information — solves Threat 1.
 - (a) Block all network access on computer, except to exam website.
 - (b) Block all access to file systems (files on computer, but also on dongles, etc.).
 - (c) Block all access to non-exam material & communication on exam website.
2. Controlled access to the exam attempt — solves Threats 2-4.
 - (a) Block access to the exam outside the exam period.
 - (b) Block access to the exam outside the exam location.
 - (c) Block transferring or sharing access to the exam (attempt).

If a threat cannot be eliminated, it should at least be detected.

5 General Solution Approaches

5.1 Access to Information and Examination

Several general options are available to control access to the information, communication, and the exam:

1. A *physical token* only at the exam location required for the duration of the exam attempt.
 - (a) In its simplest form: a *paper* exam, preferably graded automatically (with e.g. Auto Multiple Choice). This addresses all threats, but it is not computer-based.
 - (b) A university-owned and controlled *dongle* coupled to the student's computer (bring your own device, BYOD). This is *our Examiner solution*. Every student receives a dongle at the opening of the exam, cannot take it outside the exam location, and returns it when leaving. It is described in more detail in the next section. It addresses all threats.
 - (c) A university-owned and controlled computer for each student at the exam location. The Examiner dongle can be used in this setup too. It addresses all threats.
2. *Common unshareable secret*. In essence, a password to enter the exam (Oncourse quiz) that the student does not know. *The invigilator types in the password* on the computer of the student. This method does not address Threat 1, access to disallowed information (including communicating with others). Students must be at the exam location, and cannot share the secret. However, it does not prevent leaving early and continuing the attempt outside.[†] We've used this approach as a fall-back for students for whom the Examiner dongle did not work. It works well with up to say 15-20 (non-dongle) students per invigilator.
3. *Common shareable secret*. Essentially, a password to enter the exam that the student knows. We've used this approach a number of times, for students with time extension that started the exam early, and as a fall-back for students for whom the Examiner dongle did not work. Experience shows that this *does not work at all*: as soon as the password is e.g. written on the backboard, it is immediately communicated to outside the exam location by mobile phone. Moreover, this method does not address Threat 1 access to disallowed information (including communicating with others). Note that the Safe Exam Browser's exam key (.seb file) is a common shareable secret, with the problems just described.
4. *Personal shareable secret*. For example, a personal code given to each individual student. It has to be filled in as part of the exam, and *the leaving time of the student has to be recorded when leaving early*. This method does not address Threat 1 access to disallowed information (including communicating with others). But it allows a semi-automated check that there is no activity on the exam (attempt) after leaving.[†] Note that it does not make sense for the student to share the code because multiple

attempts with the same code will be visible in the system, clearly flagging a problem. We've used this approach a number of times as a fall-back for students for whom the Examiner dongle did not work. It seems to work, in the sense that we have not seen activity after leaving early.

5. As the Examiner, but *booting over the network*. Since it is not a physical token it does not address all threats, even when used in combination with secrets.

First, note that *only paper-based exams and the Examiner dongle solve all threats* listed in Section 3. In particular, none of the other methods restrict access to the Internet, or stop sharing access to the examination attempt with another person.

Second, note that all methods have an accompanying exam protocol, i.e. how to distribute, use, and return, the dongles, passwords, personal codes, and so on. We return to the protocol complexity as a cost measure later.

Finally, regarding text marked with [†]. Except for paper and dongle-based exams, the exam protocol should include asking students to show on their computer that they have submitted their exam before leaving. This solves the problem of continuing an attempt after leaving early. Clearly, this is only an issue for (formal) exams where students can leave early.

5.2 Impersonation

Threats 7 and 9 of Section 3 are partially due to impersonation, i.e. someone other than the student takes the exam. At intermediate exams, the student's identity is not checked. Moreover, with any of the methods described below, any person can take an attempt, pretending to be a given student. At formal exams, the student's identity is checked by an invigilator, but this identity check is not correlated to the student's (own) identification at the exam website. The student is thus free to take an attempt for someone else. The essence of this problem is that a student self-identifies at the exam website (during the exam period at the exam location), and that this identification is not checked.

With the Examiner dongle we can observe that the same dongle is used to make multiple attempts (the dongle ID is linked to an IP address, which is coupled to an attempt). For this reason we regard this threat to be minor because it does not make sense for a student make someone else's attempt but not his or her own.

5.3 Collaboration

Most threats can be solved independently of the exam website. However, disallowing sharing access to the exam (attempt) strongly depends on the behaviour of OnCourse. In particular, OnCourse (in fact, Moodle) allows:

1. Multiple browsers (i.e. students) with same or different IP addresses to simultaneously work on the same exam attempt.
2. Closing a browser (and computer) without submitting an attempt, and returning to the attempt from (another) browser or computer.

None of the solutions described above eliminate these scenarios. Although note that the Examiner dongle ensures these scenarios can only take place during the exam period at the exam location. While we cannot prevent these threats (examples of Threats 7 and 9 of Section 3), *we can (automatically) detect them in the Oncourse log files* if the web accesses to a single attempt have different IP addresses, which is very likely. (Only if multiple attempts are behind a NAT, or if the student manages to keep the IP address from within the exam room to outside, or fortuitously re-associate to the same IP address, would this not be the case.)

5.4 Overview

The table below collates the above analysis. A dash entry indicates that the threat is not applicable to this column (thus and threat is solved by the column). An X entry indicates that this column does not address this threat (thus that the threat is still to be solved by another column). Notes:

1. Except for paper exams, we assume that a dedicated exam.oncourse.tue.nl website is used for exams (instead of the oncourse.tue.nl website for “regular” Oncourse website), thus eliminating some threats. We have only shown the exam.oncourse server column for the Examiner, but its advantages are duplicated in the three “secret” columns. The exam.oncourse.tue.nl website only contains exams, and no other course material. It is also not possible to send messages or post to fora.
2. We assume that the exam protocol asks students to show that they closed the attempt to the invigilator (in formal exams).
3. This is not necessarily a problem, and we have allowed this in the past.
4. Cloning, modification, and impersonation are technically hard to do. We could detect modifications by check-summing the dongle during the exam. Cloning and impersonation are very likely to be detected. We can detect that more dongles are used than have been handed out, or because the original and clone are used at in the same exam. *It is currently (easily) possible to impersonate the dongle at the exam.oncourse.tue.nl website, but eliminating this is planned in the short term.*
5. Check that there was no activity on the attempt after the recorded leaving time. This is not required if item 2 is implemented.
6. See Section 5.2. Note that multiple attempts by the same dongle can use different IP addresses. Without a dongle, it would only be possible to observe that different attempts from different IP addresses are in fact be from the same computer if we ask the ICT department for the Exchange account using that IP address at that particular point in time. For this reason, the remainder of the row is listed as “not detected.”
7. See Section 5.3.
8. We assume that the Safe Exam Browser uses a common shareable secret.
9. In our experiments (Section D), we found several ways to access files or Internet during use of the SEB.
10. The only difference between Examiner and network boot is where the

boot image resides: on a memory stick or on the network. The column can be interpreted as replacing the Dongle column in the Examiner solution. We assume that no secrets are used.

	physical token		Examinator ¹ exam.oncourse server	Examinator server	network boot ¹⁰	common unshareable secret ¹	common shareable secret ¹	personal shareable secret ¹	Safe Exam Browser
Threats	paper	dongle				password	password	personal code	
file systems	-	blocked			blocked	X blocked	X blocked	X blocked	partial ⁹ blocked
Oncourse information	-	blocked	blocked			X	X	X	blocked
network access, Google, etc.	-	blocked			blocked	X	X	X	partial
networked communication	-	blocked			blocked	X blocked	X blocked	X blocked	partial? blocked
oncourse communication	-		blocked						
share attempt with others in room	-		detected ⁷			detected ⁷	detected ⁷	detected ⁷	detected ⁷
share attempt with others outside	-	blocked			X	blocked ²	detected	detected	detected
others at exam do attempt	-		detected ⁶		X	X	X	X	X
others do attempt outside	-	blocked			X	blocked	X	X	X
never enter, entire attempt outside	-	blocked			X	blocked	X	blocked	X
leave early, entire attempt outside	-	blocked			X	blocked ²	blocked ²	blocked ²	blocked ²
continue attempt outside	-	blocked			X	blocked ²	blocked ²	blocked ²	blocked ²
wrong dongle nr	-		detected	detected	-				
same dongle nr	-		detected		-				
stolen/lost dongle	-			blocked	-				
reused dongle	-		detected ³		-				
cloned dongle	-			detected ⁴	-				
modified dongle	-			detected ⁴	-				
impersonate dongle	-			detected ⁴	-				
wrong personal code	-			-	not detected				
share personal code	-			-				detected depends	-
Effort									
pre exam	print exam	-	-	upload config	-	-	-	print	-
entrance	distribute	distribute -	-	-	-	unlock	broadcast	distribute	distribute
during	-	-	(check logs)	(check logs)	-	-	-	-	-
exit	collect	collect, check ²	-	-	-	check ²	check ²	check ²	check ²
post exam	(get) grade	integrity check	get results	get grades	-	-	-	check activity ⁵	-

6 The Examiner

We first define the operation of the Examiner dongle, followed by how it is used for formal exams and intermediate exams. We then discuss a few additional issues that have to be taken into account.

6.1 Operation

In this section we describe how the Examiner dongle works. In essence, the dongle is a USB stick with a very restricted Ubuntu linux distribution. Students power down their laptop, insert the dongle, and then boot from the USB stick. It works for all university-supplied laptops of the previous six years, as well as many (but not all) other laptops. Unless only university laptops are supported, fall-back methods must be provided. We return to this later.

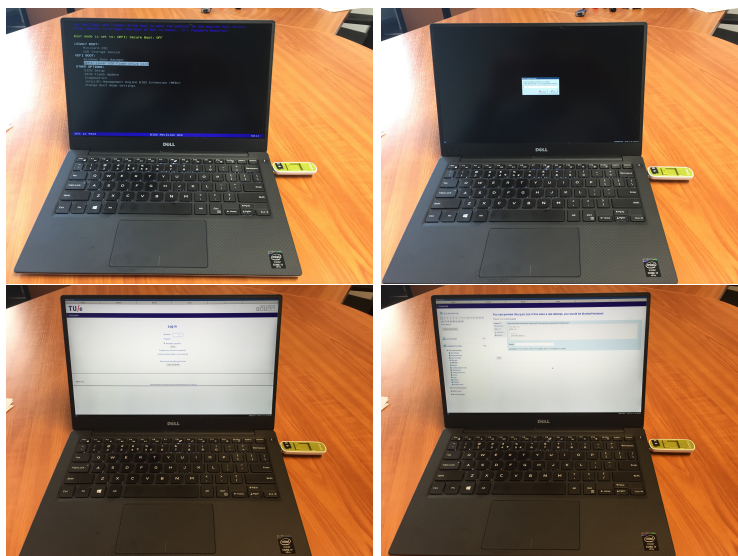


Figure 2: The Examiner dongle inserted on the right-hand side of the laptop. Top left: booting (D in Fig. 3); top right: TUE WPA2 network login (E in Fig. 3); bottom left: Oncourse login (G in Fig. 3); bottom right: Oncourse quiz.

Since students boot their laptop from the dongle, all network and file access is handled by the dongle. In particular, the dongle only allows use of the TUE WPA2 network to access only the dedicated `exam.onscourse.tue.nl` website (for the exam) and the Examiner server. More precisely, the Examiner server is contacted first, to receive the list of allowed websites and the exam key that is required to start the exam. Figure 1(b) illustrates the effect of using the dongle.

Figure 3(b) illustrates the technical protocol used by the Examiner dongle, the Examiner server, and the Oncourse website. The protocol uses and

extends the Safe Exam Browser (SEB) protocol, which is shown in Figure 3(a).

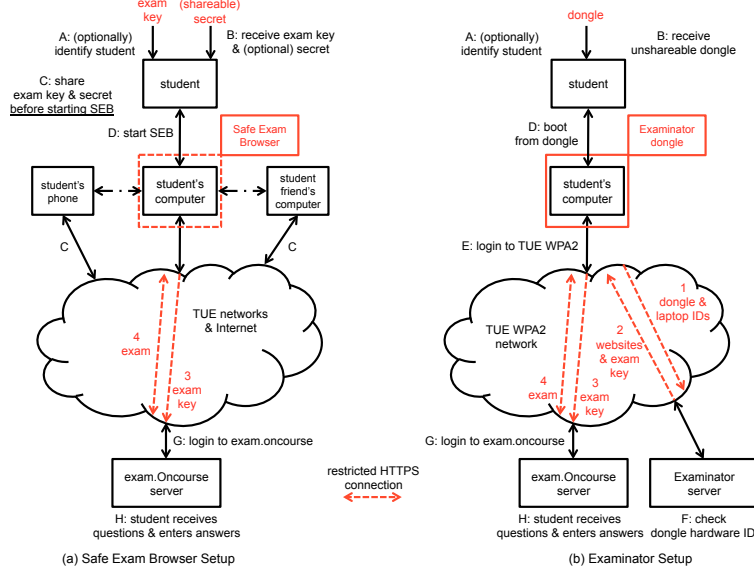


Figure 3: Protocol used by the Safe Exam Browser (a), which is extended by the Examiner dongle (b).

We describe the SEB protocol first, followed by the Examiner protocol. The SEB is a software program (a browser) that the student runs on his or her computer, after downloading it from a public website (safeexambrowser.org). After starting, the SEB (aims to) restrict the use of the computer to connecting to the exam website only. This is achieved by sending the *exam key* (which is specific to a particular exam) to the exam website, which checks the exam key. Oncourse (Moodle) has a special SEB plugin to achieve this. The problem is that the exam key is a small computer file that has to be distributed to students before or at the start of the exam, and in any case before entering the exam website. As a result, the exam key can be shared by students before starting the SEB (and thus before locking the computer). To avoid this, the SEB allows the use of a password to unlock the exam key. However, since it is a common shareable secret, this merely delays sharing (see Section 5.1).

The Examiner protocol uses the SEB exam key and the SEB Oncourse plugin too. However, the student is only given a physical (unshareable) token, namely the dongle. The dongle blocks the student's computer (cannot access file system or network) and contacts the Examiner server over a secure connection. After having been authenticated on the basis of its hardware identifier, the dongle receives the exam key. From this point onwards, the SEB protocol is

used. Because the student never receives the exam key it cannot be shared. This, and the fact that the dongle is an unshareable physical token, make the Examiner solution safer than the SEB.

Using the Examiner protocol, but booting from a network image instead of a USB stick is shown in Figure 4. The main difference is that there is no physical token, which allows more threats. Moreover, the TUE network has to support hundreds of students downloading the boot image at the start of the exam, which may be problematic. The boot image server may be the same as the Examiner server or different.

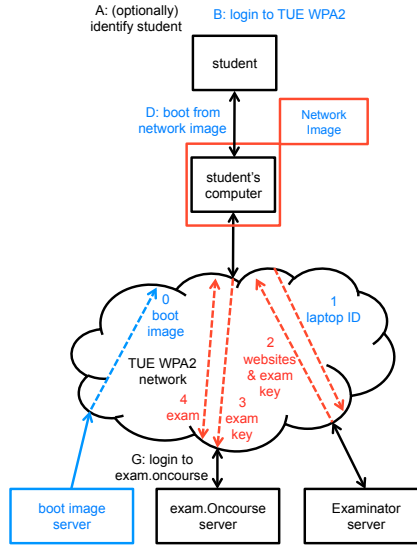


Figure 4: Examiner protocol, but using Network Boot instead of USB stick.

6.2 Ideal Scenario: Formal Exam

In this section we describe the protocol of a formal exam when using the dongle:

1. Pre-exam.
 - (a) Create the exam as a quiz in Oncourse.
 - (b) Standard settings are to be applied. In particular: define opening and closing times for the exam, set number of attempts to 1, set automatic submission at close of exam, restrict network access to the TUE WPA2 network, and restrict the browser to be the Safe Exam Browser. No password is required.
2. Exam.

At each exam the following must be present:

 - (a) A dongle for each student.
 - (b) For each student, instructions on how to use the dongle. They can

either be projected, given out on paper, or be omitted if students are familiar with the setup. Instructions we have used in the past are included in Appendix F.

These are the steps to be followed (in a lot of detail!):

- (a) As students enter, hand out a dongle to each (and remind them they need to return it).
 - (b) Students sit down and start laptops with dongle, preferably before the exam opens.
 - (c) When the exam opens (as indicated in the quiz settings), students can enter the exam.
 - (d) One of the questions in the exam asks for the unique dongle number, as label-printed on the dongle.
 - (e) When students finish they should submit their attempt.
 - (f) If students finish before the end of the exam period, and are allowed to leave early, then *they must show an invigilator that they have submitted their attempt* before returning the dongle and leaving.
 - (g) When the exam closes, as indicated in the exam settings, all open attempts are automatically submitted.
 - (h) Student return their dongle as they leave. Or dongles are collected before they leave.
3. Post-exam.
- (a) The exam is graded either automatically by Oncourse or else manually. Optionally, download Oncourse grade and response overviews.
 - (b) The Examiner server has a list of hardware IDs of all dongles that were used in the exam. Each ID is linked with the corresponding dongle number, IP addresses, and MAC address of the network card of the laptop(s) that used it. (It could also be extended with the Exchange account name used to login to the TUE network.)
 - (c) The Oncourse exam has a list of dongle numbers as entered by the students. Investigate any missing, duplicate, or incorrect numbers.
 - (d) All dongles that were taken to the exam are checked for integrity. This also spots any missing dongles. (Checking *all* exam dongles eliminates false positives for missing dongles.) If missing dongles were used in the exam, find out which student it was. *Blacklist* the hardware ID of any missing dongles: they cannot be used in future exams.
 - (e) Download Oncourse log file for the exam. (Semi-automatically) check that no student used more than 1 IP address. Assuming that the student had no network or dongle problems, this suggests fraud.

We use template instructions for students and invigilators; these are included in the Appendices.

6.3 Ideal Scenario: Intermediate Exam

A formal exam and an intermediate exam differ in that the latter takes place in a normal lecture room or notebook room. As a result students are not allowed

to enter late or leave early. The protocol for the Examiner dongle remains the same, except that item 2f when students finish early, is replaced by

- If students finish early, they shutdown and close their laptop, and do nothing for the remainder of the exam. This includes not playing with their phone.

With some practice, students adhere to this rule. In our experiments, see Section D, we've asked students to return the dongles after the exam, without asking them to leave the room. This has worked well, in the sense that we've not lost any dongles.

6.4 Scenario: Students with Time Extension

Students with a time extension are (percentally) a growing group. They can be dealt with easily in formal exams by extending the closing time of the exam to include the time extension. This doesn't really work for informal exams where it is hard to force the remaining 95% of students to be quiet while a small group still works. The converse works better: start the time-extension students earlier.

This requires that two exams are made that are identical (just duplicate them in Oncourse), except for the opening time. After the exam, it must be checked that only students that are allowed a time extension did that exam.

6.5 Scenario: Non-Dongle Students

As mentioned above, the dongle does not work on all laptops. As a result, one of the suboptimal methods (cf. Section 5) must be used. We have tried pretty much every combination.

For formal exams, we have used the *common unshareable secret* (the invigilator types in the exam password) and the *personal shareable secret* (code). Both work fine, but recall that students have access to information and communication on the Internet. We tell students that they are not allowed to have any application other than the web browser, which can only have one window with one tab. On a (moderately) positive note, because all Oncourse exam pages (of all students) look very similar, it is very easy to spot a different web page in a sea of laptops. (And we have.)

For informal exams, we have used the *common shareable secret*, i.e. just an exam password. This is woefully inadequate, and actively circumvented.

6.6 General Considerations

The combination of a single exam with and without dongles, and with and without time extension students *requires four Oncourse quizzes*. Although identical in terms of questions, they do require different quiz settings. Since they are modified manually, this increases the scope for errors.

It is highly recommended to have a practice quiz with students where they can try out the dongle, and see if their laptop works with it. The large majority

of students were not unwilling to use the dongle, but a subset of students essentially did not want even try (for potential fraud or other reasons). Since our courses included practica, we forced everyone to try the dongle in a practicum.

The success of the Examiner dongle (i.e. reduction in work) (inversely) depends on the absolute number of students that do not use it. It is therefore essential limit the fall-back scenario to only those students are really require it.

7 Cost-Performance Analysis

Computerised examinations may be desirable for various reasons, including the same format for Oncourse home work and exams, allowing students to (re)do exams later as (automatically-graded) homework or practice exams, allowing students to inspect their attempts after grading (this is a big advantage), and so on. If allowed by the type of questions of the exam, automated grading is clearly the most important advantage.

The various options introduced above have different costs (in terms of work and purchase cost) and performance (which threats are addressed). In particular the following costs are relevant (although we do not quantify all):

1. Complexity of use for students.
2. Complexity of use for invigilators.
3. Complexity and amount of work required by staff before, during, and after each examination.
4. Purchase cost of dongles.
5. Purchase and maintenance cost of university-owned and managed computers (excluding Oncourse servers and Examiner server).
6. Cost (FTE, know-how) of development, maintenance, and deployment for Electronics Systems Group only.
7. Cost (FTE, know-how) of TUE-wide development, maintenance, and deployment for TUE as a whole.

We assume the cost of making the exam questions to be the same for all methods. In terms of performance we consider:

1. Which threats are addressed (eliminated, detected, not detected).
2. For what percentage of the student population.

We consider the following solutions, which may have to be used in combination:

1. *Traditional manually-graded paper exam.* High cost of grading. Otherwise cheap. Maximum performance.
2. *Traditional manually-graded paper exam automatically exported by On-course (Moodle)* To be used in combination with the Examiner. As above. Several efforts are reported here

(https://docs.moodle.org/29/en/Quiz_FAQ#Is_there_a_nice_way_to_print_a_copy_of_a_quiz.3F).

If we can adopt one of these solutions with little effort (as expected), this reduces cost, at equal performance. Currently we manually convert On-course exams to a paper exams, with the risk of making mistakes.

3. *Traditional automatically-graded paper exam.* Low cost, including that of grading. Maximum performance. The major disadvantage of this approach is that the kinds of questions that can be asked are much reduced compared manually-graded paper exams and also compared to Oncourse. In particular, even numeric answers are painful (at least in Auto Multiple Choice, <http://home.gna.org/auto-qcm/index.en>).
4. *Automatically-graded paper exam automatically exported by Oncourse (Moodle).* To be used in combination with the Examiner. This significantly reduce cost, at equal performance. However, see note above. This option is operational, and can be found at https://moodle.org/plugins/view/mod_offlinequiz. The Mathematics and Computer Science Faculty have a similar solution.
5. *Oncourse and Examiner with BYOD.* Higher cost than paper exams in terms of complexity of use in the exam. Low maintenance cost per exam (resetting/reflashing the dongles after each exam takes about 30 seconds per USB stick, or 3 hours for 500 sticks). The main cost, which is hard to gauge, is that of organisational development and deployment. Cost of dongle is low (2.8 euros). Performance is almost as high paper exams.
6. *Oncourse and Examiner with university-supplied computer, as fall-back in exams with BYOD.* In other words, students whose laptop does not work with the dongle get a university laptop during the exam. Compared to the previous bullet, a cheap laptop, such as Chromebook, is required, costing around 250 euro. Note that they are only required for a subset of students. Performance as above.
7. *Oncourse and Examiner with university-supplied computer, as only option in dedicated exam rooms with only these computers.* As above, but requiring dedicated examination rooms, which seem to be in short supply. Performance as above. This option is deployed at a number of universities. Examples include <https://it.umn.edu/exam-security> and those listed at <http://eassessment.eduhub.ch/scenarios.html> (look for "institutional hardware scenario" category).
8. *Oncourse and common shareable secret.* Low cost. Low performance, i.e. it is very easy to cheat. For this reason this option can only be recommended as a fall-back. (Performance improves slightly with the use of an EXAM VLAN.)
9. *Oncourse and common unshareable secret.* Slightly better performance than the previous bullet, but slightly higher cost in terms of exam protocol complexity.
10. *Oncourse and personal shareable secret.* As previous bullet, but more post-exam work to check for fraud.

A qualitative overview of the costs and performance is shown in Figure 5. The arrows indicate a range of cost or performance, which depends on the percentage of students not using the dongle. For formal exams, Examiner dongle BYOD + paper manual grading is a good trade-off of cost and performance. For intermediate exams, instead, the least bad solution seems to be the Examiner dongle BYOD with a personal code (personal shareable secret).

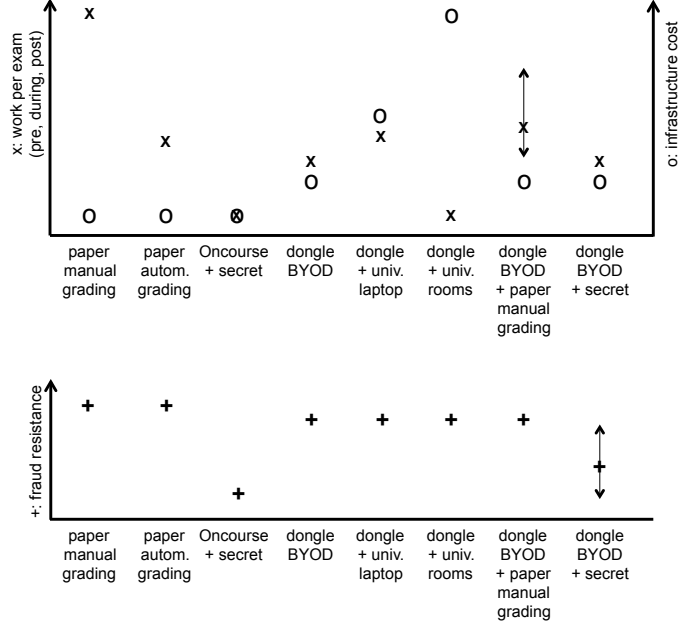


Figure 5: Approximate relative Costs and Performances.

7.1 Recommendations

For formal exams we would use, in decreasing order of preference:

- Examiner (5) + university computers in dedicated exam rooms (7) (possibly long-term, highest cost, best performance)
- Examiner (5) + university laptops (6) (feasible, medium cost, best performance)
- Examiner (5) + paper exam generated by Oncourse (2) (planned, low purchase cost, higher protocol cost, best performance)
- Examiner (5) + paper exam (1) (deployed, low purchase cost, higher grading cost, protocol cost as above, best performance)

For intermediate exams we would use, in decreasing order of preference:

- Examiner (5) + common shareable secret (9) (deployed, low purchase cost, low protocol cost, good+bad performance)
- Examiner (5) + university laptops (6) (feasible, medium purchase cost, medium protocol cost, best performance)
- Examiner (5) + paper exam generated by Oncourse (2) (deployable but not planned, low purchase cost, higher grading cost, protocol cost like above, good performance)

We have spent several person-months developing the Examiner solution. It is hard to quantify the cost of maintenance and deployment, especially TUE-wide.

8 Conclusions

This documents reports on the investigation into the use of computers to enter answers to examinations, without increasing the risk of fraud compared to a paper examination. We have designed a dongle-based solution that allows students to use their laptops in intermediate and formal exams. We successfully implemented and deployed this Examiner solution in a number of intermediate and formal examinations, with up to 350 students at a time, spread over several examination rooms.

The Examiner works for the vast majority of students, but the remaining 5-10% require a fall-back solution. Three options seem appropriate: paper exam, university-supplied laptop only as fall-back, or university-supplied computer for all students.

Given this proof of concept the following questions arise:

- We are not aware of better solutions, but the state of the art should be investigated.
- It needs be decided if the Examiner is a starting point for wider deployment in the TUE, possibly after further development.
- If affirmative, it needs be decided who is responsible for further development, deployment, and support. The authors's are strongly of the opinion that university-wide infrastructure should be developed, deployed, and maintained by the university, not individual faculties or groups. As a side note, even though the faculty of Mathematics and Computer Science offer excellent support for Oncourse and PEACH, the above remark also holds for Oncourse, PEACH, and content servers (e.g. for content too large to fit on Oncourse or other university systems).
- Given that the Examiner solution seems to be unique in what must be a wide-spread need, deployment outside the university may be of interest. Intellectual property rights should then be investigated, and a (business) plan defined. (As an aside, the Safe Exam Browser rejected this option, according to their September 24 2015 presentation.)

The Examiner solves an acute problem for the Electronic Systems group, and will continue to be developed and deployed for internal use until answers to the above questions are clear.

9 Acknowledgements

First of all, we thank all the students of Computation (5EIA0 and 5AIA) who in their first quartile of their first year, patiently endured our experiments. Next, we would like to thank the Oncourse team, Jan Willem Knopper and Hans Cuyper for their excellent support, and willingness to install various plugins.

A Terminology

1. An *examination* is offered to one or more students. We use the term exam for both the collection of questions, and for the process of giving/taking the exam.
2. We distinguish *intermediate* exams that take place in a normal lecture room from *formal* exams that take place in a exam room according to official examination rules (including identification, invigilation, arriving late, leaving early, toilet visits, etc.). We assume that the former do not allow arriving late, and do not allow leaving early. They may allow starting or finishing at multiple times; especially the latter is useful for time extensions.
3. There may be multiple *versions* of the same exam. (In particular: different numbers for the same calculated question, different variants of the same question, different orders of a set of questions).
4. When *attempting* an exam, a student receives a version of the exam, and can enter answers to questions. Multiple attempts of the same exam by a single student may or may not use the same exam version.
5. An attempt is *submitted* is when it is irrevocably marked as finished. This happens at most once, and should happen exactly once. Oncourse/Moodle can automatically submit at the end of the exam period.
6. The exam *period* is the time period during which the exam may be attempted, from opening to closing. All attempts are started and finished within the exam period.
7. The exam *duration* is the maximum time allowed for a single attempt. The duration is not longer than the period.
8. Exam *location*. E.g. dedicated examination room with invigilators (for formal exam), lecture room or notebook room (for intermediate exam).
9. *BYOD*: bring your own device. Students use their own laptop in the exam. Alternatively, the university supplies the computer.
10. *Dongle*: a university-owned and managed USB stick that the student has to insert in the computer to take an exam.
11. Each Examiner dongle has a unique *hardware identifier* (ID) that cannot be changed.
12. Each Examiner dongle has a unique *number* indicated by a printed label on the stick.
13. The exam *protocol* is the sequence of steps that students and invigilators have follow to take and give an exam, respectively.

B Oncourse Evaluation

Oncourse (more generally, Moodle) works well as an environment for learning:

1. Oncourse works well as a repository for content (slides, software, etc.). Much better than OASE.
2. Oncourse works well for online lectures with embedded flow control etc.

- that force students to do a sequence of steps (e.g. read text, watch video, do quiz, upload results).
3. Oncourse works well for ungraded homework and tests that can be made at home (quizzes). Note that we do not care about copying, fraud: this is the student's responsibility.
 4. Oncourses question banks, randomisation, etc. work well. (Although its a lot of work.) There are some issues with sharing questions between courses; in particular with visibility of questions for (non-editing) teachers, etc.
 5. Oncourse works well to analyse student behaviour, e.g. grades, participation. We have much more insight into how much (or little) students do. For example, we have observed that in later weeks, one students follows an online lesson, to get the assignment at the end of it. One student makes the assignment, and identical answers (e.g. computer programs) are uploaded within a short time frame by multiple students. It is clear that students who have not take the online lesson cannot have received the assignment, and should not be able to upload it.
 6. Oncourse works well for polls, e.g. to find out what students think about certain topics.

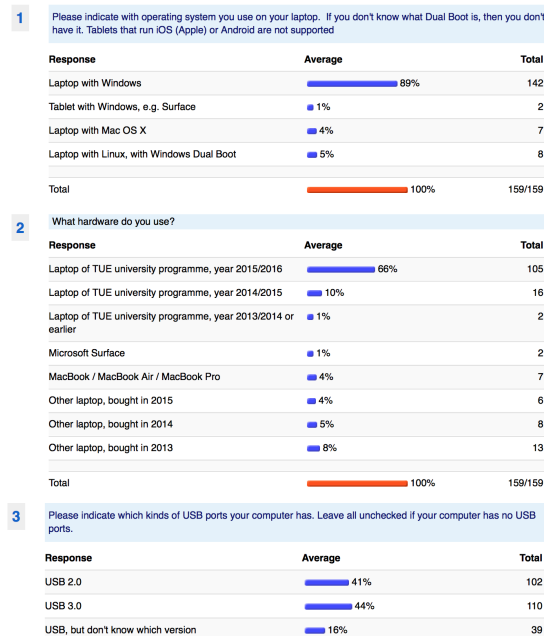


Figure 6: Example poll, related to the use of the Examiner dongle.

7. LaTeX support is good, although the resulting images can be slow to load.
8. Oncourse works well with certainty-based learning, and ok with certainty-based marking.

9. The TUE Oncourse infrastructure has handled our examinations with 350 students at the same time without problems.

However, Oncourse cannot handle:

1. Not all Oncourse quiz/exam results include the student number. This means that a manual step is required to add student numbers. Moreover, the list of enrolled students in Oncourse is not necessarily the same as the OASE list or the examination list provided by the administration. In all cases, error-prone and time-consuming excel manipulation is required to post-process data.
2. Large content (videos, screencasts, large software, models) can in theory be hosted on Oncourse. In practice, this makes Oncourse backups very large, and there is a limit to the backup size that can be restored. For this reason, we this content must be hosted elsewhere. We host it on its own servers, but should be university servers. It should not be on YouTube, etc. This is known to the Oncourse team, who, like us, use their own TUE servers for their content.
3. Oncourse works for peer reviews, but not in combination with groups.

Oncourse does not work as an examination environment. Major issues:

1. Students can access all content in Oncourse during exams, including material of the course but also other courses.
2. Students can communicate using messages, fora, etc. in Oncourse during exams.
3. Multiple browsers (i.e. students) with same or different IP addresses to simultaneously work on the same exam attempt.
4. Closing a browser (and computer) without submitting an attempt, and returning to the attempt from (another) browser or computer.

The first two bullets we resolved by using a restricted `exam.oncourse.tue.nl` website. The second two bullets have been discussed in Section 5.3.

C Examiner Dongle

We have the following requirements for the Examiner dongle introduced in Section 6:

1. Works on most hardware from the past 15 years, including laptops from the past 1-2 years that use secure boot.
2. It can be easily customized to only contain a limited set of software.
3. Large repository of software is available.
4. Running from a read-only file system.
5. Run locally, to avoid a heavy load on the network infrastructure.

From these requirements, a Linux live CD/USB stick was the only viable option. The first version of the dongle is based on the Ubuntu live CD. We briefly describe the changes that we made, starting with the removal of features that were not desired:

1. Remove installer and all special boot targets.
2. Disable login/password on all accounts.

3. Disable console login.
4. Remove all auto-mount tools.
5. Remove unneeded software.
6. Remove login manager.
7. Cripple the network manager and disable all network devices.

Next, we added:

1. Firmware and drivers for most modern wireless network cards.
2. A graphical environment with a very limited desktop that gives access to a pre-defined set of tools.
3. Custom wireless connection scripts.
4. A python re-implementation of the safe-exam browser.
5. A bootstrap script that contacts the examiner server.

The rest of the Examiner setup pertains the examiner server. When the dongle has finished booting, the student is asked to enter his or her Exchange username and password, which are used to set up a connection with the TUE WPA2 wireless network. Once the connection has been established, the Examiner server is contacted for a setup script. This script validates the dongle stick hardware identifier and the laptop MAC address with the server, sets up the network routes and hosts entries based on a list of approved servers. If the validation succeeded it starts the exam browser with the obtained exam key and opens the configured Oncourse website. This script can be easily extended to add security features or allow access to extra tools.

D Experiments

1. The Electronic Systems group has moved to Oncourse as a teaching environment, i.e. without its use in intermediate or formal examinations for a number of courses: 5EIA0, 5AIA0, 5KK03 (5LIB0), 5AIC0, 5LIC0, 5LIS0. These include bachelor and master courses in all years. We use Oncourse to disseminate lecture material (slides), readers, screencasts; home work (quizzes); do web polls; send emails to all course participants (in fora); students upload projects. We are very satisfied with Oncourse.
2. We used the *Safe Exam Browser* with Oncourse (with SEB plugin) for one formal exam (5KK03) in a supervised exam location with 3 MSc students. SEB damaged two student computers running Windows 10 to such an extent that complete re-installation of Windows 10 was required. This, and the fact that SEB is often very slow in loading web pages, and can be bypassed (on Apple computers with user switching), led us abandon the use of the SEB.
3. We used Oncourse for the formal exam of 5KK03, in an examination location with invigilators for about 20 MSc students who had never used Oncourse before. We did not use any anti-fraud measures (rustig toetsen, SEB, Examiner, exam.oncourse.tue.nl, passwords, etc.). We detected

one case of fraud (Googling during the exam), which was reported to the examination committee.

4. We used Oncourse five times for intermediate examinations of 5EIA0 (in AUD 3, 250 students) and simultaneously 5AIA0 (in AUD 6, 100 students). The exam rooms are very suboptimal: tightly packed location, no spacing between students, no good surveillance.
 - (a) Week 2: we did not use any anti-fraud measures (rustig toetsen, SEB, Examiner, exam.oncourse.tue.nl, etc.) other than a common shareable secret (password given to students in the room). We only restricted access to the exam to the TUE network. This caused problems for a number of students that had no TUE network access (because they hadn't set it up correctly). Cheating & copying took place at a large scale. We did not offer a longer intermediate exam for students with a time extension. Students had difficulty being quiet during the exam, and when finishing early.
 - (b) Week 3, we used the Examiner for a subgroup of students with the same settings as in week 2, except that we used the TUE guest network (since it requires no login). Students were better behaved, with much less cheating. For the other students who did not use the dongle, we had a non-dongle exam, with the same setup as in week 2. We did not offer a longer intermediate exam for students with a time extension.
 - (c) Week 4 as week 3, but we additionally offered longer intermediate exam for students with a time extension, by starting them early on a separate password-protected quiz.
 - (d) Week 5 as week 4, but all 350 students used the dongle. Many students were not able to connect to the TUE guest network. It seemed that the local routers would only allow 255 concurrent connections.
 - (e) Week 6 as week 5, but we changed the dongle to use the TUE WPA2 network. This required an additional login step (to WPA2 network, as well as to the Oncourse server). This worked well for the vast majority of students.
5. We used Oncourse and the Examiner dongle for 5AIC0 (third-year bachelor) formal exam with students who had only tested the dongle once in class, but had not used it for (intermediate) exams before. We used a personal code for the students that could not use the dongle. We used the TUE WPA2 network, and had no network problems. 20 students with dongle, 8 students with personal code. We had paper exams as fall-back, but these were not used. We had two quizzes: one with dongle, and one without. No separate time-extension quiz was required.
6. We used Oncourse and the Examiner dongle for 5LIC0 (second-year master) formal exam with students who had only tested the dongle once in class, but had not used it for (intermediate) exams before. We used a personal unshareable secret, i.e. the invigilators typed in the password on

student computers. This worked well. We used the TUE WPA2 network, and had no network problems. About 80 students with dongle, 10 students with personal code. We had paper exams as fall-back, but these were not used. We had two quizzes: one with dongle, and one without. No separate time-extension quiz was required.

7. With some trepidation we used Oncourse and the Examiner dongle for the formal examinations of 5EIA0 (in Studyhub, 230 students) and 5AIA0 (in Paviljoen J17 and L10, 90 students). We used the dongle, with the oncourse.tue.nl website, the TUE WPA2 network. We used a personal code for students who could not use the dongle, and a paper copy of the exam (manually graded) for students without a laptop. 5AIA0: 85 students with dongle, 6 students with personal code, 1 with paper exam. 5EIA0: 202 students with dongle, 31 students with personal code, 3 with paper exam. Each course had two quizzes: one with dongle, and one without. No separate time-extension quiz was required. We did not find any evidence in the log files that students with a personal code, and who could access the exam after leaving, did access their attempt after leaving. We used the course instructors, who were trained in the Examiner exam protocol to distribute and collect dongles and personal codes. The university invigilators were pleased with the new examination protocol. We had no problems with network connections dropping in J17 and L10, but had a few problems in Studyhub. One student started with the dongle but finished on paper, and another student vice versa.

E Technical Recommendations

Examiner recommendations, in decreasing priority:

1. As mentioned previously, our current Examiner dongle does not implement the exam key. To impersonate a dongle at the exam website it is therefore enough to pretend to be the SEB using browser spoofing. We plan to address this soon.
2. The Examiner dongle and the TUE network are not always stable, and it should be investigated what the cause of this is. See the experiments for examples.
3. The Examiner servers should also log the Exchange account name used to login to the TUE network, to facilitate some of the fraud checking without requiring information from ICT. We can then also eliminate asking students for the dongle number, since it can be derived. (For psychological reasons it may still be good to ask for the number though.)
4. Ideally, the dongle would only use a dedicated TUE examination VLAN that only allows access to a restricted set of IP addresses (including the Examiner server and the exam.oncourse.tue.nl server). The substantial benefit is that students that do not use the Examiner dongle then cannot use the Internet or disallowed TUE websites/information. (They can still

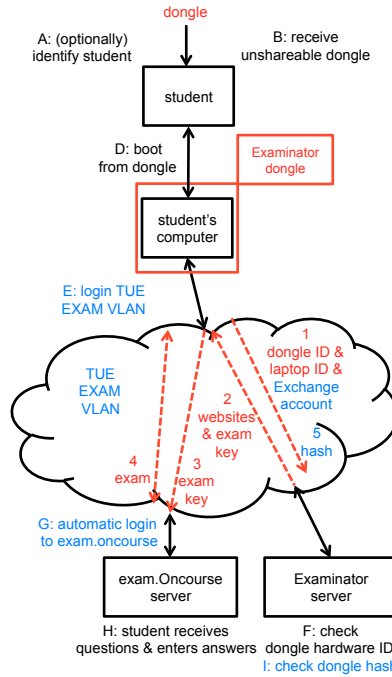


Figure 7: Improved Examiner Protocol. Modifications shown in blue.

set up computer-phone and computer-computer networks, as well as access files on their computer). Moreover, an EXAM VLAN removes the threat that a student logs in using the TUE VPN. The EXAM VLAN could be restricted to certain locations and/or periods, and should be Exchange password protected to allow for comprehensive logging.

5. A “single sign-on,” i.e. ideally, a student scans his or her identity card with the camera on the laptop, and is automatically logged in on both the WPA2/EXAM network, and on the exam server. This removes the threats described in Section 5.2.
6. Although we do not consider it a major threat, it would be possible to check-sum the dongle image while the student is using it, and send the resulting hash to the examination server. Any cloning or modification of dongles would then be detected.
7. Although we have focussed on the use of the Examiner dongle to only access the exam website, it can potentially be used for programs other than a web browser. In particular, the dongle already contains a calculator, but we could add more programs such as C programming environment Eclipse or a modelling environment. This would allow students to develop

programs, models, etc. on the computer without access to the Internet or their own files, before uploading them to the exam website. We will investigate this next academic year for the 5EIA0, 5AIA0, and 5LIS0 courses that include C programming.

Oncourse (Moodle) recommendations, in decreasing priority:

1. Simultaneous access to the same attempt with different IP addresses is already partially detected and should be blockable. Since the IP address is logged by Oncourse, this should not be hard to implement. This removes the threats described in Section 5.3.
2. It should not be possible to return to an open attempt after closing the browser, which is a problem for non-dongle exams. This would simplify the exam protocol by not having to ask students to show that they submitted their attempt. This removes the threats described in Section 5.3.

However, note that this feature is (and has been useful) when the network connection is lost during the exam. Students can then continue their attempt.

F Student Instructions

Instructions for Students to take an OnCourse Examination with or without USB Stick (v0.4)

1. Make sure that you get an examination USB stick from the invigilators.
If in the past you could not use the USB stick with your laptop, then ask for a piece of paper with a personal code instead.
2. If you have a personal code, go to step 9.
3. **Shut down** the laptop (not standby but full shutdown).
4. **Insert** the examination USB stick in a USB port.
5. Start the laptop and directly press and **hold down the boot menu key** (often tapping it repeatedly gives the best result).
 - a. HP: F9
 - b. ACER, DELL, Lenovo: F12
 - c. MSI: F11
 - d. Apple: ALT/option
6. **Select the USB stick** in the option menu. e.g. USB HDD; for Apple UEFI boot.
7. When the pop-up window appears, **login** to the wireless network (e.g. s234351 and password, same as for OnCourse).
8. Wait until a browser appears.
9. **Login at OnCourse**, go the right course, and start the examination
 - a. “exam with USB Stick” when you have a USB stick, or
 - b. “exam with Personal Code” when you have a personal code.
Ask an invigilator to enter the **password** for the examination.
10. Finish the examination by **submitting** it in OnCourse.
11. If using a USB stick, **push** the power button to shut down the laptop. **Unplug** stick.
12. Hand in your USB stick or piece of paper with personal code when leaving the room.

USB Stick Options

You can use the following key combinations when using the USB stick

- Reset wireless : windows-W or ALT/option-W on Mac
- Calculator: windows-C or ALT/option-C on Mac
- Close open window: control-Q

In the browser you can zoom in and out with + and -. You can also go back to the OnCourse home page, reload page, etc. with the buttons at the top of the screen.

In case of problems

First, don't panic. We guarantee your grade never suffers due to technical problems.

- If OnCourse hangs or you have lost the WiFi connection then reset the wireless with windows-W or ALT/option-W (Mac).
- If all fails, call an invigilator.

All activity is logged, including IP addresses. USB sticks are traceable to you. Any activity in the OnCourse examination after leaving the exam will be detected, and invalidates the examination.

G Invigilator Instructions

Instructions for invigilators to manage an OnCourse Examination with or without USB Stick (v0.2 – small group)

We assume the examination is in a controlled examination setting, and not e.g. an intermediate examination in a normal lecture room. We assume that the student group is not too large for the invigilators to type in the password for all non-USB students.

In the examination room must be available

1. **USB stick** for each student.
2. For each student, **instructions** on paper on how to use the USB stick.
3. A paper list of **personal codes** to be given to students who cannot use the USB stick.
4. A **password** to enter the Personal Codes examination: **do not give it to students!**
5. Optional: as a backup, a **paper examination** for each student.

Basic idea

- Everyone uses the **USB stick**. They cannot use the internet.
- Only students who cannot, get a **personal code**.
 - They must be **supervised extra** carefully, because their internet is not blocked.
 - If they leave early it is essential that **their leaving time must be noted** down.

1 - Start of Exam

When students arrive in the examination room

1. Give them the paper instructions.
2. Ask them if they have (successfully) used a USB stick before.
 - a. If yes, give them a USB stick. Tell them that they have to return it after the exam.
 - b. If no, tell them to go to the desk / invigilator that hands out personal codes.

2 - Students with Personal Codes

At least one invigilator hands out personal codes. It is strongly suggested to do this at a separate desk at the front of the room. Each code is random and unique. The personal code sheet looks like this:

Personal code	Tear here	Personal code	Student name	Leaving time
8456238		8456238	S. Johansson	13:22
52354233		52354233		

1. Write down the student name next to an unused code. Shown in green above.
2. Tear off the piece of paper with the code (shown in yellow) in the Tear Here column.
3. Tell the student to fill in this number in the OnCourse exam.
4. Tell the student that they must return to the invigilator to **register their leaving time, if they leave early**. Otherwise the exam is invalid.
5. Tell the student that when (s)he has logged into Oncourse, (s)he must ask **you to type in the password to enter the exam**. Do not give the password to students.

Reserve part of the examination room for students that use personal codes.

3 - Students that leave early (before regular examination time, or during time extension)

- Get the student's USB stick, or
- They have a personal code: Ask if they registered their leaving time. If not, send them to the invigilator / desk. Register their leaving time in the last column (shown in blue, above). **This time registration is essential to catch students continuing the exam outside the room.**

4 - End of regular examination, or end of time extension

- Get the students's USB stick, or
- No action required if they have a personal code.

USB Stick Options

You can use the following key combinations when using the USB stick

- Reset wireless : windows-W or ALT/option-W on Mac
- Calculator: windows-C or ALT/option-C on Mac
- Close open window: control-Q

In the browser you can zoom in and out with + and -. You can also go back to the OnCourse home page, reload page, etc. with the buttons at the top of the screen.

In case of problems

First, tell students that we guarantee their grade never suffers due to technical problems.

- If **OnCourse hangs or students have lost the WiFi connection** then reset the wireless with windows-W or ALT/option-W (Mac). The status of the WiFi is shown at the bottom right of the screen.
- If all fails, shutdown the laptop.
 - Remove USB stick. Take USB stick with you.
 - If there are **no backup paper examinations**, then give the student a personal code, and tell them to do the examination via the regular OnCourse.
 - If there **are backup paper examinations**, then give the student one of these.
- If everything fails (including no paper backups), then ask the responsible lecturer for a solution.

Background information

- The USB stick solution is very safe: it blocks all internet and wireless access, and access to files on the computer.
- The **Personal Code solution is very unsafe**: it does not block internet, wireless, google, email, etc. As a result students with Personal Codes must be separated in the room, and **supervised extra carefully**.
- All activity is logged, and USB sticks are traceable to students. Any activity in OnCourse after leaving the exam will be detected and invalidates the exam.