Exploring a solution for secured high stake tests on students' personal devices

Citation for published version (APA):

van Meeuwen, L. W., Verhagen, F. P., & den Brok, P. J. (2017). Exploring a solution for secured high stake tests on students' personal devices. In D. Joosten-ten Brinke, & M. Laanpere (Eds.), *Technology Enhanced Assessment 19th International Conference 2016* (pp. 171-180). (Communications in Computer and Information Science; Vol. 653). Springer. https://doi.org/10.1007/978-3-319-57744-9_15

DOI:

[10.1007/978-3-319-57744-9_15](https://doi.org/10.1007/978-3-319-57744-9_15)

Document status and date:

Published: 12/06/2017

Document Version:

Accepted manuscript including changes made at the peer-review stage

Please check the document version of this publication:

- A submitted manuscript is the version of the article upon submission and before peer-review. There can be important differences between the submitted version and the official published version of record. People interested in the research are advised to contact the author for the final version of the publication, or visit the DOI to the publisher's website.
- The final author version and the galley proof are versions of the publication after peer review.
- The final published version features the final layout of the paper including the volume, issue and page numbers.

[Link to publication](#)

General rights

Copyright and moral rights for the publications made accessible in the public portal are retained by the authors and/or other copyright owners and it is a condition of accessing publications that users recognise and abide by the legal requirements associated with these rights.

- Users may download and print one copy of any publication from the public portal for the purpose of private study or research.
- You may not further distribute the material or use it for any profit-making activity or commercial gain
- You may freely distribute the URL identifying the publication in the public portal.

If the publication is distributed under the terms of Article 25fa of the Dutch Copyright Act, indicated by the "Taverne" license above, please follow below link for the End User Agreement:

www.tue.nl/taverne

Take down policy

If you believe that this document breaches copyright please contact us at:

openaccess@tue.nl

providing details and we will investigate your claim.

Exploring a solution for secured high stake tests on students' personal devices

dr. ir. Ludo W. van Meeuwen, Floris P. Verhagen, prof. dr. Perry J. den Brok.

Eindhoven University of Technology: De Rondon 70, 5612 AP, Eindhoven,
NL

L.W.v.Meeuwen@TUE.nl

Abstract.

Digital testing requires software and hardware. A hardware option is to establish dedicated test halls. As an alternative, this paper describes a setup and first experiences of a pilot run on a proof of concept, to answer the questions: which conditions are needed to create a secure solution for high stake assessments via students' personal devices (e.g., notebook from students)?

To answer this question, a proof of concept was run based on an outline of a Secure Test Environment Protocol (STEP). This STEP was based on three shells of security: Prevention, Detection and Reaction. Prevention concerns the technical solutions to prevent the use of unauthorized sources during tests. Detection concerns the risks (i.e., chance and impact) and the possibilities to detect unauthorized behavior and security issues. Reaction gives insight in requirements needed for an organization when students' personal notebook are being used in taking high stake tests.

The preliminary conclusion from the proof of concept is that it is possible to use students' personal notebook in secured high stake tests if a STEP - comprising three shells of security - has been implemented. Suggestions for further development are given.

Keywords: Security in digital tests, Bring Your Own Device, Controlling students' personal notebooks, Secure Test Environment Protocol.

1 Introduction

The access to specific software during testing is becoming a necessity to pursue an optimal validity of a test in the curriculum of a university, such as Eindhoven University of Technology (TU/e) as the focus of the present contribution. If for example the learning objectives of a course comprise the use of software (e.g., Matlab, SPSS), the software should be made available for students when they take the test of the course; when a large amount of writing is required to answer questions, text editing software can be

more efficient (e.g., typing is faster than writing, digital editing is easier, grading is easier), etcetera. In line with findings of SURF [1, 2], Teacher experiences at the university show that students should be provided a secured digital test environment to avoid access to communication software (e.g., Skype, desktop sharing, drop-box, e-mail) and to avoid unwanted access to data on the hard disk and/or on the internet. Monitoring only seems insufficient to avoid fraud in digital assessment. The literature suggests four conditions to optimally prevent students to commit fraud: 1. the boundaries of what is acceptable should be communicated to the student, 2. situations conducive to fraud should be avoided (e.g., secured environment in digital tests), 3. Test situations should be monitored so cheating during testing can be detected, and 4. In the event of fraud, sanctions should be imposed [3, 4, cf. 5, 6, 7].

In order to create a secured digital testing environment, several educational institutes (e.g., in the Netherlands) established test halls equipped with computers that are fully run by the institute (e.g., University of Utrecht, Delft University). Next to the advantages (e.g., more experiences in the field, easier technology), the establishment of such halls are known to have disadvantages: The rooms are hardly or not available for other purposes than taking tests (hence, during testing period in use only), the investment and operational costs are high, and scaling is difficult in case of fluctuating (e.g., increasing) numbers of students.

Therefore, the desire of educational institutes is to use the students' personal device (i.e., notebook) more than in the current situation is the case. However, little knowledge is available about using students' personal notebooks during high stake tests [8, 9].

This paper explores a solution for secured high stake tests using students' personal devices to answer the questions: *which conditions are needed to create a secure solution for high stake assessments on students' personal device (e.g., notebook from students)?* Therefore this paper first introduces the three steps of a Secure Test Environment Protocol, based on an earlier performed desk research [8]: 1. Prevention, 2. Detection, 3. Reaction. Next it describes the experiences of a pilot run of a proof of concept [10]. Finally, the conclusions are drawn, based on the evaluation of that pilot.

2 Three security shells

Obtaining one hundred percent safety during high-stakes testing is an illusion. Therefore, the aim is to obtain an optimal Secure Test Environment Protocol (STEP). Such a protocol comprises three steps or shells (Figure 1) [8, 11, 12]:

- 1. Prevention: Options for committing fraud should be averted as much as possible by the institution,
- 2. Detection: It should (pro-actively) monitor - known and potential - security leaks and last but not least,

- 3. Reaction: the institution should react when a security leak has been found or has been suspected.

Figure 1 three security shells for a complete STEP: 1. Prevention, 2. detection, 3. reaction.

3 Creating a controlled test environment on students' notebooks in shell one

The first step is to create shell one; how can students' personal notebooks be configured in such a way that basic security for STEP can be obtained?

3.1 Controlling students' notebooks

The use of personal notebooks implies that students can 'prepare' their notebook in order to by-pass security and/or monitoring software during testing. The prevention of such fraud during tests, starts with controlling the personal notebooks during tests. This control can be called the inner shell of the secured digital test environment.

An estimation of risks is needed to be able to define the best optimal solution for the notebook configuration during tests. Risk is defined as chances for fraud by the impact of the fraud. Impact can be *very high* (e.g., taking tests from outside the test hall), *high* (e.g., full communication possible), *medium* (e.g., extra information available via internet), or *relatively low* (e.g., access to local hard drive/limited information). The estimation of chance is depending on the a. skills from a cheater needed to modify the computer for cheating, b. time needed to cheat during the test, and c. time needed to invest prior to the test [8]. Verhagen and De Hesselle [13], made an estimation of the risks for fraud for mainly two scenarios (i.e., standard notebook with WiFi available and without WiFi).

There are almost endless possibilities when using software to by-pass security control, but there are possibilities to drastically reduce these options too. Hence, the design of the secured environment on personal notebooks (i.e., shell one) aims at diminishing these options. Taking control as early as possible in the booting process has the highest success rate (i.e., the later in the process, the more options and less complicated knowledge is required to by-pass security) [8]. Figure 2 outlines the booting process of a computer in four steps: First, the Video card, system board, and RAM memory are being addressed (i.e., BIOS start). High level computer knowledge is needed to change this part of the booting process. Verhagen [8] estimates that even students on a university of technology will be challenged to by-pass this process during testing, rare exceptions excluded. Second, the computer storage will be accessed to start the operating system (step 3; e.g., Windows) that allows applications (step 4; e.g., a browser) to run.

Figure 2 boot sequence.

Changes in storage, operating system or applications are easier to make and easier disguised. For example, a lock-down browser is an application that allows students to only have access to the test server. Because 'preparation' of a personal notebook is possible, manipulation by use of scripting within the storage or operating system could make it possible to have access to other applications while using the lock-down browser in such

a way that detection by monitoring software is unlikely. In the event of additional network monitoring to such security solution, students could avoid detection of their fraud (e.g., by using other Wi-Fi connections like smartphones). Therefore, control over the personal notebooks should be taken over right before the moment the notebooks' storage is activated. The use of a virtual machine makes it possible to virtually imitate a physical machine. In theory, this could make it possible that the boot, controlled by the institution, is running on an operating system that is controlled by the student with all potential possibilities of fraud that can be imagined. It is hard for applications to detect the use of a virtual machine. However, Linux® has possibilities of detecting all the common virtualization programs.

3.2 Technically three options

The study by Verhagen [8] was focused at the situation of the TU/e where approximately 85% of the Bachelor Students are using the same sets of notebooks, selected each year by the institution. This allowed the focus for the pilot to work on the small variety of notebooks that the majority of the students have.

Figure 3 outline controlled test environment on personal notebooks.

The institutionally controlled test environment on the personal notebooks should continue the boot process from the moment that the notebooks' storage would be addressed

(see Figure 2). Three options were defined for high stake tests to get an institutional controlled operating system (and applications) running on personal notebooks during tests.

1. Option A: Boot image via UTP (wired) network, hence wired connection with boot- and test server.
2. Option B: Boot image via USB-stick, connection with test server (wired or Wi-Fi) (Figure 2).
3. Option C: Boot image via Wi-Fi, hence, connection with boot- and test server via Wi-Fi

Solutions A, B and C are similar as they all use the idea of a boot image that takes control over the personal notebooks. The difference is the way of distributing the image to the notebooks: A. a wired connection, B. a USB-stick, and C. via Wi-Fi.

Next to their risk analysis, Verhagen and De Hesselle [13] made an estimation of the potential control of the situation when the options A, B, and C (e.g., including the USB-stick solution) compared to the use of a lock-down browser.

In short, options A, B and C are almost equally secure. Option C. was excluded: The Wi-Fi capacity will not be sufficient in the coming few years to allow large groups of (say approx. 300) students to simultaneously download their secured image (including the download of software as Matlab or SPSS). Option A. was excluded too: A wired connection with a boot server means preparing a test-hall with wired internet connections and the installation and connection of several boot servers. The aim of this study was to avoid such investments. Option B, with the boot image via a USB-sticks and Wi-Fi connection to the test server turned out to be the best solution (Figure 3). A proof of concept has been set up and described by Goossens and Koedam [10] using a Linux image on a 2-Euro USB-stick.

4 Detection and reaction

The USB-solution prevents students to use their notebooks for (non intended) communication during tests. As mentioned above, next to prevention, also detection and reaction are crucial aspects of a secured environment [11, 12]. In the desk research [8], prevention, detection and reaction are shown as three shells of the secured environment (Figure 1). The inner shell represents the technical solution like solutions A, B, and C, mentioned above. The second shell represents the detection and the third shell represents the reaction.

4.1 Detection; shell 2

The proctor will be an important factor in the security of tests. The security of the USB-solution is only useful when test taking takes place in a secured test hall. Monitoring increases chances of being caught when committing fraud and can help in detecting security leaks. This implies that proctors should be trained to be able to detect fraud in a digitalized situation. Furthermore, they should check for (wireless) connections (e.g., smart phone, smart watch, dongle) like they do with paper based exams. However, these

checks are not at all security proof since the existence of a broad spectrum of wireless communication protocols.

A continuous way of monitoring using (HD) camera's is expected to work in a preventive way, and can make it easier later on by the examination committee to determine whether suspected fraud has occurred or not.

Logging the network traffic can be useful. However, experience shows that analyzing the logs can be a labor intensive job. So large scale network logging particularly is useful when the logs can be analyzed automatically. Preferable, notifications of suspicious network-use are generated automatically.

4.2 Reaction; shell 3

"For the detection process to have any value there must be a timely response" ([11], P.5.). This implies that ownership and processes must be arranged in case of security attacks [12]. These attacks could come from both inside and outside the organization. However, for now we focus at the danger from inside the organization (i.e., attempts of fraud by students).

The standard procedures in cases of fraud in paper based tests should be applied for digital testing too. In case of detection this means: writing an official report, safeguard the evidence (e.g., time stamps for data logs and video recordings, screen casts, etc.), communicating the case to the institutional body that is responsible for deciding on sanctions (e.g., examination committee).

In case the security of the first shell has been penetrated, an investigation should always be done in order to inspect the damage of the shell and plan reparation and improvement of the shell. This is not the task of an examination committee. This task should be assigned to the "owner" of the digital environment (e.g., software, hardware, regulations, and procedures). The impact of a single student that bypasses security is high, but easier to control than a scenario where a more general by-pass of the security is found that can work for a large group/all students.

Independent of fraud prevention, it is important to reduce the possibility for students to rationalize fraudulent behavior. A cat-and-mouse-game will probably start if prevention of fraud would be rule based only. An approach could be to express trust to students that they will become a scientist that will follow the rules of scientific integrity. At the same time tell them that acting against the rules on testing, will violate that trust [6].

5 Pilots

Pilots were run to test the solution with students [14]. Two pilots were run in April 2016 in two exams at the Eindhoven University of Technology. The characteristics of the courses were chosen as diverse as possible. One course was from the Electro Engineering department dealing with embedded systems design. The other course was dealing with Academic Writing in English, and could be followed by all students.

For both pilots, a Moodle environment (i.e., OnCourse) was used as online test suite. The Electro Engineering assessment comprised multiple choice questions and short answer questions. The English course assessed the students by using two open questions with an open text field for the students to write their answers.

In total, 135 students were assessed. 102 students (76 %) used a windows notebook from the TU/e notebook arrangement. 33 students used another notebook. All students (100%) were able to make and successfully send in all their answers of the test. The number of successful test administration using the USB-stick was 104 (77%). The others (23%) did not use the memory stick to boot their notebook but went to the test environment by using their normal browser. Extra monitoring by proctors secured these exams. The reason for not being able to use the USB-stick was diverse (e.g., students not willing to use the solution, exotic notebooks that did not boot from the stick, and problems with Macs). At the time of this pilot the main reason for not being able to boot from the memory stick was a sudden problem with almost all Macs.

From the evaluation it was learned that overall students perceive the digital assessment with the USB-stick as all right but that they are worried about a situation when technology fails. Teachers are happy to use digital assessment as the correction work is easier and faster.

5.1 Conclusions and recommendations from the pilot setup for further development

The proof of concept that was used in the pilot is described in detail by Goossens and Koedam [10]. Here we sum the main advantages and disadvantages. Starting with the first:

- The USB-stick solution by Goossens and Koedam [8] is in line with analysis above. Control is taken over early in the booting process of the students notebooks. Possibilities for students to 'prepare' their notebook for cheating are limited (i.e., in institution control)
- The USB-stick itself is a physical token with a unique hardware ID. This allows the use of black/white listing of these tokens as part of the STEP security measures.
- The USB-stick solution allows the use of Wi-Fi so the establishment of test halls with wired connections is not necessary. The secured environment only allows the network card to connect with the safe test server (or other trusted environments where software can be run).

Some disadvantages to deal with are:

- There is no guarantee that all notebooks can boot from the USB-stick. However, this can be known on forehand, tested and possibly be solved per occasion.
- The notebook market should continuously be monitored for changes, to avoid (groups of) notebooks that suddenly do not work. A practical implementation is to check all student notebooks at the start of the academic year. But still sudden changes in the BIOS could have impact on the performance.

- Software (e.g., Matlab, SPSS, Word) are not available yet on USB stick due to several challenges (e.g., licenses, suitable for Linux, stick size)

The main recommendations for the STEP solution, based on the pilots are focused at the further development of the solution. For further development it is important firstly to arrange the ownership of the solution in the organization to insure a fast reaction in case of security problems and/or problems with functionality (e.g., sudden failure of the solution on all Macs). Then there is the need to improve the procedures prior and during the assessment and communicate the procedures to all stakeholders (e.g., students, proctors) and focus at the teachers' needs for essential software in assessment (e.g., SPSS, Matlab),

6 Preliminary conclusion and discussion

Based on the reports [8, 10] and the experience from the pilots [14], the estimation is that the use of personal devices (i.e., notebooks) in taking high stake tests is possible (as inner shell of a complete STEP solution). The core of the solution is a (Linux) boot from a USB memory allowing Wi-Fi connection to the test server only. However, for the time being, the solution only seems to work in a situation with a homogeneous selection of devices (i.e., notebooks) including a need for an individual test of students notebooks prior to their first exam. In addition, there is the continuous need to prevent and to detect the use of virtual machines. A secured test environment should be created (i.e., STEP, shell 2) where attempts of fraud can be detected. Last but not least, the organization should arrange a third shell (i.e., shell 3), that arranges the passage of cases of fraud and arranges the reaction in a more technical way when fraud and a leak in shell 1 and 2 have been detected. This shell should also comprise an owner of the system who is responsible for the continuous testing procedures that are necessary to prevent a sudden failure of (groups of) notebooks that should work with the USB boot.

Acknowledgement

We wish to thank all colleagues and students who made it possible to run the pilots. In particular thank to prof. dr. Kees G.W. Goossens, ir. Martijn L.P.J. Koedam, Rob C. F. van den Heuvel, and ir. PDEng Huub M.P. de Hesselle for sharing their knowledge.

References

1. SURF (2014). Richtsnoer veilige digitale toetsafname [Guidebook secure digital assessment]. SURF, Utrecht. The Netherlands.
2. SURF (2016). Werkboek veilig toetsen [Workbook secure assessment]. SURF, Utrecht. The Netherlands.
3. Bloothoofd, G., Hoiting, W., & Russel, K. (2004). Plagiaatbeleid aan de Universiteit Utrecht, faculteiten en opleidingen [Plagiarism prevention at the Utrecht University, departments and programs]. Utrecht, the Netherlands.

4. Duggan, F. (2006). Plagiarism: Prevention, practice and policy, *Assessment & Evaluation in Higher Education*, 31, 151-154.
DOI:10.1080/02602930500262452
5. Park, C. (2003). In other (people's) words: Plagiarism by university students - literature and lessons. *Assessment & Evaluation in Higher Education*, 28, 471-488. DOI:10.1080/02602930301677
6. Van Meeuwen, L. W. & Kraak, I. T. C. (2015). *TU/e educational fraud policy*. Eindhoven University of Technology. The Netherlands.
7. Rienties B., & Arts, M. (2004). Omgaan met plagiaat: Van intuïtie naar bewijs [*Dealing with plagiarism: From intuition towards evidence*]. Tijdschrift voor Hoger Onderwijs, 4, 251-264.
8. Verhagen, F. (2015). Mogelijkheden gecontroleerd digitaal toetsen [Possibilities secured digital assessment]. Eindhoven University of Technology. The Netherlands.
9. SURF (10-11 december, 2015). Digitaal toetsen, ga er maar aan staan [Digital assessment, the challenges]. Utrecht, The Netherlands.
DOI:<https://www.surf.nl/agenda/2015/12/tweedaags-seminar-digitaal-toetsen-ga-er-maar-aan-staan/index.html>
10. Goossens, K. G. W. & Koedam, M. L. P. J. (2016). *Fraud-resistant computerised examinations*. ES Reports, Eindhoven University of Technology, The Netherlands. DOI:<http://www.es.ele.tue.nl/esreports/esr-2015-03.pdf>
11. LaPiedra, J. (2000). The information security process prevention, detection and response. *Global Information Assurance Certification Paper*, 1-6.
DOI:<https://www.giac.org/paper/gsec/501/information-security-process-prevention-detection-response/101197>
12. Schneider, B. (2014). The future of incident response. *IEEE Computer and Reliability Societies*, sep/okt, 95-96.
DOI:https://www.schneier.com/blog/archives/2014/11/the_future_of_i.html
13. Verhagen, F. P. & De Hesselle, H. M. P. (2016). *Risicoanalyse digitaal toetsen via BYOD* [Risk analysis digital assessment in BYOD]. Eindhoven University of Technology. The Netherlands.
14. Van den Heuvel R., Van Meeuwen, L. W., Verhagen, F. P. (2016). Pilot beveiligd toetsen TU/e [Pilot secured assessment TU/e]. Working group pilot 'secured assessment'. Eindhoven University of Technology. The Netherlands.