Securing the ICT-based examination

Petter Gysler Bjørklund

Master's Thesis
Master of Science in Information Security
30 ECTS
Department of Computer Science and Media Technology
Gjøvik University College, 2010

Avdeling for
informatikk og medieteknikk
Høgskolen i Gjøvik
Postboks 191
2802 Gjøvik

Department of Computer Science
and Media Technology
Gjøvik University College
Box 191
N-2802 Gjøvik
Norway

Abstract

This master project covers security aspects related to conducting ICT-based examination of students. We have investigated security requirements and best practice of conducting examination in a digital environment. We have tested and performed security analysis of existing solutions and we have developed a framework based on the requirements and the findings in the security analysis. We have also looked into the implementation possibilities to support the theory behind the proposed framework.

It is crucial to establish some security measures in order to trust systems that earlier was done with pen and paper. Many solutions does not address these issues adequately and the expenses of commercial proprietary solutions is not always justified by the level of security they yield. For this reason we focus on the use of open-source software and projects for the framework and solutions. The project contributes by providing a framework which will help increase the level of security in current examination systems and systems that will be developed for ICT-based exams, and at the same time it will hopefully help with cutting expenses in these implementations by using free and open source software.

Sammendrag

Masterprosjektet dekker sikkerhetsaspekter relatert til utøvelse av IKT-basert eksaminering av elever. Vi har undersøkt sikkerhetskrav og beste praksis rundt det å utføre eksaminering i et digitalt miljø. Vi har testet og utført sikkerhetsanalyser av eksisterende løsninger og vi har utviklet et rammeverk basert på kravene og funnene i analysen.

Det er avgjørende å opprette visse sikkerhetsmekanismer for å kunne ha tillit til systemer for eksamen som tidligere ble utført med penn og papir. Mange løsninger konfronterer ikke disse sikkerhetsutfordringene på en tilfredstillende måte og kostnaden med å implementere kommersiell og propreitære eksamensapplikasjoner rettferdiggjøres ikke alltid med tanke på sikkerhetsnivået som de holder. På bakgrunn av dette vil prosjektet fokusere på bruk av åpen programvare og prosjekter for rammeverket og eventuelle løsninger. Masterprosjektet bidrar ved å tilby et rammeverk for sikkerhet i IKT-basert eksamen som vil hjelpe til med å øke graden av sikkerhet i nåværende eksamenssystemer og hos systemer som skal utvikles for IKT-basert eksamen. I tillegg håper vi skoler vil kutte kostnader i disse implementasjonene ved å bruke åpen programvare.

Acknowledgement

The results of this thesis would not be possible without the contribution of others. First of all, my supervisor Åsmund Skomedal should achieve much gratitude for the guidance and support throughout the writing of this thesis. Jørgen Ringstad have done a great job as an opponent of this thesis, and I am very thankful for all suggestions.

I would also like to give a big thanks to the 118 IT-administrators at the Norwegian high schools for completing the survey. Without you, the bigger picture of the situation would not have been obtained.

I am also very grateful for the support provided by Joshua Hesketh and Truls Fretland when they have promptly answered questions and assessment forms.

I wish to thank Frode Volden for help with some statistical viewpoints on the analysis of the survey.

Last but not least, I would like to thank classmates, friends, family and other more or less significant people who have supported me in the process of writing this thesis. You know who you are.

Contents

List of Figures

List of Tables

1 Introduction

This chapter contains a brief explanation of the topics covered in this master project, the problem description, a section about the motivation for conducting a master thesis on the subject. The two last parts of this chapter will cover research questions that will be answered by the master thesis and contributions that will be made due to this thesis.

1.1 Topics covered by the project

As technology evolves it is natural that an increasing amount of teaching and learning is performed by digital means. This project will cover an important aspect of this process, namely the ICT-based examination of students. In order to obtain trust in systems that takes part in this process, some security and privacy properties must be ensured. The project will identify these properties, as well as investigating what requirements such systems must sustain in teaching institutions in Norway today.

Based on the identified properties further work in the project will include specification on how to secure such systems, how the architecture and design of the system should be. Some analysis of how the risks are mitigated in this system will also be covered.

1.2 Problem description

Norwegian high schools[1] are instructed by the Norwegian Directorate of Education and Training[2] to conduct ICT-based examination of students. Exams should be effectuated as ”normal” exams, where they are held in a supervised environment (e.g. a classroom). This introduces new security challenges as technology literacy increases among students who may be tempted to find a way to use illegal aids in these exams. Illegal aids may include, but are not limited to: programs, files, chat sites, WiFi hotspots or wireless networks based on infrared or bluetooth technology.

To mitigate these security challenges Norwegian Computing Center have implemented a solution, called *digeks*, which utilizes booting an exam-prepared operating system from a USB memory stick. The scope of this project will be to improve the security functionality in the memory stick OS needed in an exam setting. The project will establish foundations and protocols that enforce a highly secure and controlled working environment for electronic examination and computer assisted education.

Another aspect of the problem is that students might consider implemented security mechanisms as a form of surveillance of their activities and a breach of their privacy. This thesis will also consider how privacy can best be preserved by minimizing the amount of surveillance and focusing on good security measures.

[1] In Norwegian: Videregående skoler
[2] Utdanningsdirektoratet

1.3 Justification, motivation and benefits

In a society where education is, or should be, an important aspect, the educational establishment must be trusted. One part of this trust relationship is the correctness of conducting examination of students. One can say that the ability to provide security and correctness in the context of exams says something about the quality of the school or university holding it.

Inspection of each and every machine to provide the security required in these kind of settings would be way too cumbersome and expensive. Another way to go would have been to use commercial software and tools, but this might also be very expensive and security in these systems are not always documented in a satisfied manner.

1.4 Research questions

The research questions that will be answered by this thesis is as following:

1. What is the best practice of ICT-based examination security in educational institutions today?
2. What are the prioritized security requirements for conducting ICT-based exams?
3. What security measures and protocols need to be implemented to adhere to these requirements?

The first research question:

It is valuable to gain understanding of how the ICT-based exam are conducted in educational institutions today, and how security is preserved in these environments. One way to perform this investigation would be to interview the system administrators of different schools. A considerable amount of people had to be investigated, so this solution is too time-consuming for this master project. A different approach to this research question is to conduct web-based surveys sent out to the same administrators. An advantage of this approach is that less time and money is used to achieve the desired results. Additionally, online surveys tend to get higher response or incidence rates than other methods as the respondents can choose when to take the survey. A disadvantage with this technique is that the panel integrity will not always be the best, but measures will be taken to mitigate this[3].

The second and third research question:

One assumption that is made here is that not all of the administrators or developers that will implement these kind of solutions are information security experts and thus cannot be expected to know all threats and methods to mitigate these. For this reason we will map the different security requirements worth prioritizing. We will also provide list of possible security measures and protocols to implement in the framework.

1.5 Contributions

We have in this project provided a security framework which will mitigate threats associated with ICT-based examinations. This framework is based on investigations in educational institutions which conducts ICT-based exams today and from a security analysis of existing solutions. The framework will be used as basis of improving the security in already existing solutions.

[3]Examples of measures to prevent this: `http://communication.howstuffworks.com/how-online-surveys-work2.htm`

Hopefully, the framework will also help increase the level of security in future implementations that will be used in both Norwegian high schools as well as international ones. Our adapted security assessment method, modified towards examination systems, can be used together with the proposed testing methodology as an iterative task to improve security in examination systems.

1.6 Document organization

The layout of the thesis is organized as follows: This first introductional chapter works as a preamble for the rest of the thesis and contains some information about the problem that are addressed and topics for the project, research questions are stated and motivations for the thesis and planned contributions are commented. The second chapter will address related work in this field of research, and it is divided into empirical, theoretical and privacy-oriented approaches. The third chapter will contain a survey with the purpose of investigating best practice in schools today. The fourth chapter is dedicated to explain the background for this thesis and some related theory. The following chapter will include the security analysis of the current solutions and also the results from the tests of these.

The sixth chapter will cover the various aspects of the proposed security framework for conducting ICT-based examinations. The framework proposes what protocols and security measures that will be needed to yield a certain level of security. The seventh chapter reviews the feasibility of some of the implementation parts of the framework. The last chapter includes a discussion and a conclusion of this master thesis.

2 Related work

Security and privacy concerns has emerged as a result of technological advances, especially in this case as education plays a big part in the evolution of the society. Solutions have been proposed to meet these concerns, both technical and theoretical ones. Guidelines and frameworks have been introduced to improve the security of these systems.

A good amount of research has been conducted to investigate the security implications of going from a traditional learning and examination system to an ICT-based system. Both in the theoretical area and the more practical oriented areas as well. In this digital transition there are also needs for considerations towards privacy which some has addressed.The next sections in this chapter is divided into these three ways of approaching issues in ICT-based exams.

2.1 Theoretical approaches

Most of the related work in this field have performed high-level assessment of the security and the requirements implied by the systems. The work by Marais et. al [2] are one of these which acknowledge that some criteria are met before digital exam systems should be considered secure enough:

- **Authentication;** the claimed identity must be verified
- **Location;** the assessment must be performed in the correct (and supervised) location
- **Visibility;** implement techniques that makes it hard or impossible to cheat by watching other students at the exam
- **Integrity;** ensure mitigation of electronic corruption (unauthorised modification or deletion) or double submission of tests
- **Privacy and confidentiality;** marks should be considered private information and held confidential
- **Secure client and server software;** patch systems and use a firewall
- **Non-deniability of submission;** a student must not be able to deny having taken a test

Their recommendations for these different areas of security in this scenario are mostly high-level security measures. In the integrity criteria they emphasise the importance of denying double submissions of tests and that this is not mitigated in commercial products. A solution to this problem was proposed by Apampa et al. [3] where they tie the login ID with a static IP on the computer which the assessment takes place. Thorough testing and comparative studies of this solution were not conducted and they did not consider possibilities such as source address spoofing to circumvent their solution. The work done in this thesis will certainly cover the criterias mentioned here in the process of developing the framework.

One of the earliest systems to consider security in e-learning systems are the work of the EDILE-system by Mrabet et. al [4]. It is an exam system for distance students where the students takes the exam in a supervised room with preconfigured computers. The security requirements does not go into detail, but it covers elemental security measures as integrity of exam documents, preventing cheating with illegal sources of information, authentication of students and ensure non-repudiation of answers.

Another high-level overview of security issues regarding e-learning and assessment is done by Weippl [5, 6] where he considers different security requirements and risks of the stages of an exam. Statements like "All possibilities of cheating must be anticipated and appropriate countermeasures should be prepared" is easy to make, but significantly harder to implement and measure. These high-level overviews are often a good starting point for a security framework, but we will try to look deeper into the different possibilities to cheat and suggest countermeasures to mitigate these.

Other work in this area has focused on how information security can be measured in an ICT-based e-learning system. An evaluation framework for these kind of systems have been proposed by Eibl et. al [7]. The framework consists of a catalogue of considered criteria that is build upon security pillars such as integrity, availability, confidentiality, authentication, authorization and non-repudiation. The catalogue can be considered as a check list of items which evaluation will be based on. The different items and subitems have values attached to them representing the theoretical security effect and by applying these values to a mathematical model they can be comprised to a single value between 0 and 1. The single value is based on the arithmetic mean of the security ratings s_i of each of the pillars. This security ratings can be computed as follows:

$$s_i = \left(1 - \prod_{j=1}^{n(i)} (1 - q_{i,j})^{r_{i,j}} \right)$$

Where $n(i)$ is the number of criteria considered for pillar number i, $q_{i,j}$ is the security criterion value which is in the open interval $[0;1[$ and $r_{i,j}$ is the relevance parameter of each criterion. The relevance parameter is used to describe if the criterion is applicable for the evaluated system and $r_{i,j} \in \{0, 1\}$. After computation of all pillars, the said arithmetic mean can be computed to describe the security rating of the whole system:

$$C = \frac{1}{\sum_{i=1}^{6} r_i} \cdot \sum_{i=1}^{6} s_i \cdot r_i$$

Here six pillars of security is used to achieve the final result. These intervals between 0 and 1 can be used for partitioning the different levels into named security levels. See Table 1 for an example of levels.

Table 1: Example of security level intervals

Interval	**Level**
$[0; 0.3[$	Insecure
$[0.3; 0.6[$	Low security
$[0.6; 0.8[$	Medium security
$[0.8; 1[$	High security

This method of evaluating the information security of an e-learning system is useful for this thesis as it can be used to evaluate existing solutions and can be one of the starting points of the framework developed in this project. See figure 1 for the catalogue of criteria. Some or all of the items here could be useful in an assessment process of current solutions.

Protocol-oriented approaches has also been proposed, one of these works have been conducted by Herrera-Joancomartí et al. [8] where they present a secure electronic examination protocol using wireless networks. Their model considers the devices used by the students to be trusted, so they cannot use their own equipment for the examination. Solutions to this trust problem have been confronted in work conducted by the Norwegian Computing Center [9] where they boot a secured OS from USB so the device can be considered trusted. Somewhat similar methods and software is used by Fluck et al. [10], and these approaches will be presented in section 2.2.

Another protocol-oriented approach have been conducted by two of the same researchers in the work by Castellà-Roca et al. [11] where they focus on the exam management system and how security can be obtained in the different processes of an exam. The different stages that are confronted and been the basis of the cryptographic protocols are:

1. Preparing the exam
2. Beginning, holding and submitting of the exam
3. Grading of exams
4. Obtaining the score of the exam answer
5. Revising the exam

These stages and the security requirements are used to obtain a satisfying protocol regarding ICT-based exam security. They assume that whoever implements these protocols uses a public key infrastructure to obtain certified key pairs. The relevant protocol for this thesis is mainly their protocol for stage 2:

1. TEACHER publishes exam identifier, Id
2. The STUDENT authenticates by presenting the key pair
3. STUDENT requests exam Id to MANAGER
4. MANAGER verify that the STUDENT can take the exam with identification Id. If verified, MANAGER sends encrypted (with STUDENT public key) exam to STUDENT.
5. STUDENT performs following steps:
    1. Decrypt exam and verify the content of it (by checking signatures of teacher)
    2. Performs the exam.
    3. Signs and encrypts the exam

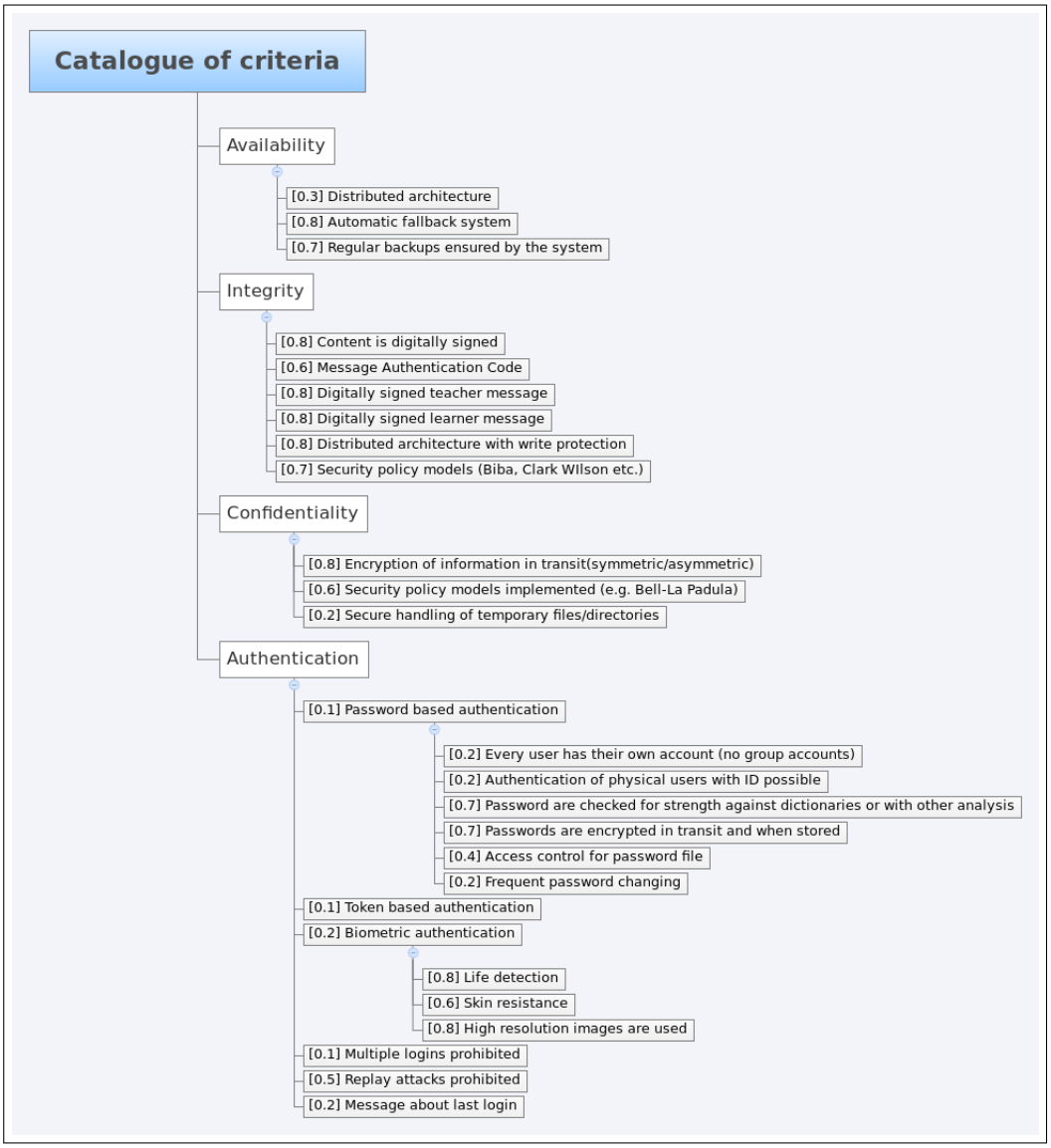


Figure 1: Catalogue of criteria

4. Sends exam to MANAGER

5. MANAGER performs following steps:

   1. Decrypt exam and verify that STUDENT have not delivered the exam before and is within given time interval.
   2. Verify digital signature of exam.
   3. Make receipt to STUDENT by signing (timestamp, Id, AnswerID) and send it to STUDENT

4. Anonymity preserved by making "masked-answer-identifier"
5. Sends signed and encrypted exam answer to TEACHER
6. STUDENT verifies signature in receipt and stores the receipt

Privacy is also considered in this approach as the teacher will not know the identity of the student while grading the exam. A trusted third party is used to achieve the privacy requirement and PKI is used to fulfil other requirements of the e-exam system. The work done in this thesis will focus on the second stage of the exam process as this is most interesting regarding security in the environment we wish to investigate, i.e. the actual conducting of the exam. It is most interesting since cheating mitigation is our primary security goal and cheating occurs at this stage.

Kambourakis et al. [12] have also conducted work in e-learning security by applying a public key infrastructure. They have considered the distance learning and how security can be obtained, and they point out that not many full-fledged security frameworks for these kind of settings exists. Another aspect they comment is that security problems such as one student passing the exam for someone else still remain, and this issue is also related to e-voting security. Controlled conditions seems to be the best environment to conduct exams. This is also the conclusion of Furnell et al. [13] in their study of security for distance learning. These mentioned supervised environments is similar to the environment in which the framework in this thesis will be developed for.

Kritzinger [14] presents a couple of good examples on how information can be compromised in an e-learning environment:

- A student could intercept another students work and resubmit it as his/her own work
- A student could receive assistance while writing the examination

The paper addresses these threats with classical information security presented earlier in this chapter and with procedural countermeasures, unfortunately with little details. This master thesis will dig deeper into these issues, but will not focus too much on the procedural countermeasures as this is out of the scope of the project.

2.2 Empirical approaches

In order to verify that some theory might be the best approach for a certain system, some empirical testing should be undergone. Related work in the hands-on department of e-learning have also been conducted, and some if it are promising and other work are a bit outdated.

Based on several protocols to provide a high level of security and privacy, Castellà-Roca et al. [11] developed an examination system to ensure their goals with the project. The system was developed and implemented in a master thesis in 2005, and in order to be as platform independent as possible the program was developed in the Java programming language. The system consists of five main components: a graphical user interface, a database containing exam-related information, a Java RMI[1] component, XML component and a cryptographic scheme component. The focus on cryptographic protocols and privacy-enhancing measures are interesting and relevant for this thesis as well, but we will also dig into other security measures that might be ap-

[1] Java Remote Method Invocation - Remote invocation of Java objects

plicable for ICT-based examinations. We will also focus on the possibility that the student might conduct the exam on their own computers, and investigate the security measures and protocols that needs to be implemented in this scenario.

To achieve a flexible and secure examination system based on ICT, Ko et al. [15] designed and developed a system which is stored on a single zip-disk. Some of the security implemented are only based on allowing white-listed physical network card addresses. The possibility to spoof these addresses are not confronted, and should have been mitigated. Internet access is not allowed, but it seems that other resources on the computer is available when running the assessment program e-Test. The system depends on cryptographic functions of the Windows operating system. Experiments in real-life scenario have been conducted in the last five years at the National University of Singapore and the deployment of this ICT-based examination system was reported to be successful. The work done here is relevant as their system considers a similar system as to what we will investigate, but some differences apply. One might be the use of zip-disks which feels a bit outdated, another is that this system is based on the proprietary cryptographic API from Microsoft. As we will investigate the use of free and open source software in this setting, this system will not be applicable for the testing phase of this master project. Another reason that this system will not be considered for testing is that the system does not seem applicable for conducting examinations on the examinees own computer.

Fluck et al. [10] presents an examination system based on a live-version of a modified Ubuntu [16] Linux installation. This system, called eExam, enables the students to use their own computers and the teachers to determine what kind of aids is allowed in a given setting. Possibilities to block several means of communication and access to own hard drive are included in the creation step of the process. The teachers are able to define a custom background image so that the invigilators easily can see if the exam candidate is using the live distribution or their own installed operating system. Bachelor degree students at the University of Tasmania has been a part of the experiment of this system and they have now conducted Australia's first ICT-based tertiary exam in 2009 [17, 18].This system will be applicable for further investigation and testing in the process of this master thesis.

A somewhat similar system were developed and implemented in some Norwegian schools by the Norwegian Computing Center [9, 19]. Whereas the system in Tasmania used Reconstructor as a tool for customising the live CD, NCC used Ubuntu Customisation Kit (UCK) to tailor a version of the KUbuntu [20] operating system. This system prevents students from accessing illegal sites and communicating with other students. Only predefined wireless access points can be used for the exam. The virtual machine threat is confronted in the research, but mitigation is done by procedural means carried out by invigilators and technical personnel. They recommend that the management part of the system should be further developed as a separate development task, as most comments after the testing period were about improvements in the invigilator system. This system will also be applicable for further investigation and testing in the process of this master thesis.

Some related work that both focuses on e-learning and security but were not relevant enough for the scenario with examinations can be found in [21, 22, 23, 24].

2.3 Privacy focus in different approaches

Privacy in this context can be viewed in two ways. Information about what the different students are doing while conducting the exam in the ICT-based system can be considered private and surveillance of their activities might feel intrusive and might in some cases also be illegal. The second way to view privacy in this setting is that identity information of an exam candidate should be preserved confidential to mitigate biased grading.

The protocol-based system of Castellà-Roca et al. [11] anonymizes the students identity, and the teacher knows that it is a valid student based on information from the trusted *Manager*. In the protocols this is performed by the manager who applies a masked-answer identifier for the examinees answers. The privacy issues tackled here is somewhat relevant for this master thesis, we want to prevent revealing the identity of the student to the person who will grade the exam answers. However, this is more or less handled by the systems provided by Norwegian Directorate of Education and Training, but where relevant, we will address these issues as well.

Weippl et. al [25] emphasises on the importance of privacy in e-learning. They identified weaknesses based on a survey they did and implemented some measures to mitigate these in an already existing e-learning system. They also found that availability and non-repudiation is more important to the students as it is expected less privacy in these kind of settings. Weippl also believes it is important to find a good balance between privacy and auditing in any e-learning system [5].

Some surveillance might however be necessary to secure the network from disruption in operation both from the outside and inside. This is especially important if wireless networks are used as attacks[2] from outside will be more available. More controversial forms of surveillance might be to monitor which applications are used and different kinds of communications that originates on the hosts of the students. We will also focus on finding the best balance between necessary surveillance and preserving the privacy in this master thesis.

[2]Examples of such attacks consists of but are not limited to dissociation and deauthentication attacks.

3 Investigating best practice

This chapter will present the process of developing a set of questions to explore how considerations are done regarding security in Norwegian high schools when conducting ICT-based examinations. The purpose is to investigate the best practice conveyed by these schools focusing on security. We will describe how sampling of the population was done as well as methods of finding the relevant contact information. The main part of this chapter is were we will present the results gathered from these investigations. We will also examine possible associations between certain variables and groups based on the results.

3.1 Investigation preperations

Valid results could not have been obtained unless questions could be properly answered. People best suited to do this in this particular situation seemed to be the system administrators of the Norwegian high schools. In order to get the desired subjects to answer our questionnaire some contact information had to be gathered, and a method for questioning these subjects had to be chosen.

A sample of the population of system administrators had to be determined, but as this population is not immensely big, we decided to send out invitations to all system administrators to participate in the survey. In this way, we avoided problems that can occur when determining a sample set of a population.

In order to collect the contact information of as many system administrators as possible, an organized list of high schools with hyperlinks to their respective home pages were used. The list [26] was unfortunately a bit outdated as the last updates were in 2005, but a more complete list was not found at the time. The method of harvesting contact e-mails is described in Figure 2.

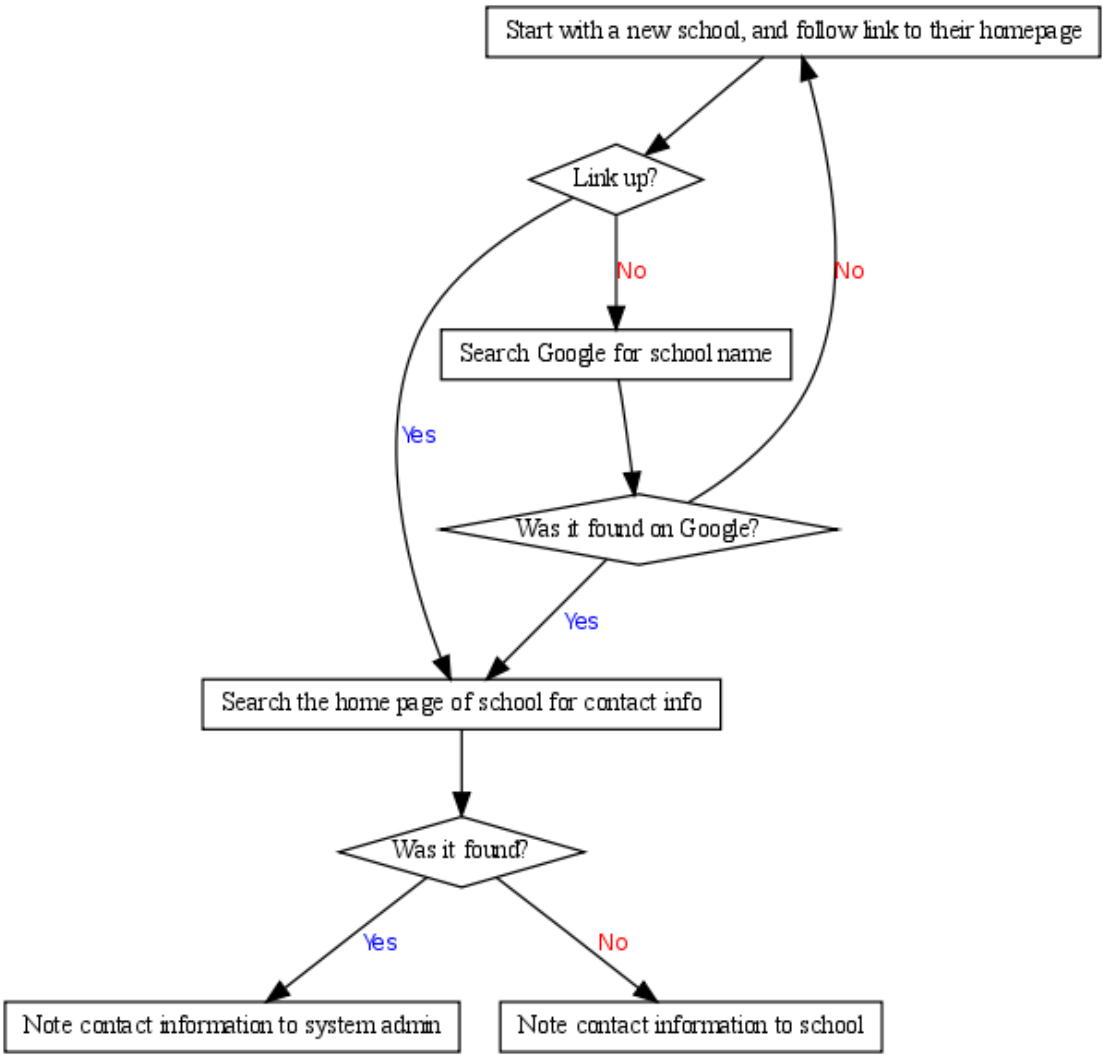


Figure 2: Search method for contact e-mail

Ultimately, 406 addresses were collected and used in the survey sent out to the different schools. All mails included information about forwarding the message to the right person if the message was recieved at the wrong instance. It was possible to answer the survey within the period of a month[1]. The english translation of the invitation sent out was as follows:

> Dear system administrator / IT-coordinator at your high school.
>
> This is an invitation to participate in a survey concerning how widespread ICT-based examination is and identify which security mechanisms that are used in these cases. If this invitation has not reached the system administrator or IT-manager of the school, it would be nice if it was forwarded to the right person.

[1] From 18th of January to the 17th of February

> The results of this survey will form a part of the result of a master degree project at the Gjøvik University College in co-operation with the Norwegian Computing Center.
>
> Respondents have the option to remain anonymous, but the identity will not be published in the final reports. It is possible to answer the survey until the 17th of February, and it takes approximately 10 to 15 minutes to answer the questions.
>
> We thank you in advance for your participation.

This invitation was initially sent out on the 18th of January and a reminder was sent out on the 10th of February. The total number of respondents ended on 118, which means that 29,1% of the invited answered, which means approximately 26% if we count with the recent population numbers of Norwegian high schools of 446 mentioned in Section 4.1.1.

3.2 Survey answers

We will in this section present the result of the survey. The full set of questions and their answering options can be viewed in Appendix A. The gist of the survey will however be discussed in the following paragraphs. Some of the questions has the "Other"-option so the respondent could write an answer that did not fit within the alternatives presented in the survey. The reason for this is to catch elements that would normally fall between answering categories. Some of the questions comes with the possibility to answer several of the choices. These questions will be marked as multiple choice questions in their respective tables.

Have your school conducted ICT-based examination?

Most of the Norwegian high schools have, as 89% of the respondents answered "Yes" to this question. The 11% that answered negatively, was asked if it was possible that future exams would be conducted this way. Only 1 person (or 7,7% in this group) answered No to that question. The rest either answered "Yes" or "There are different opinions on the matter at our school".

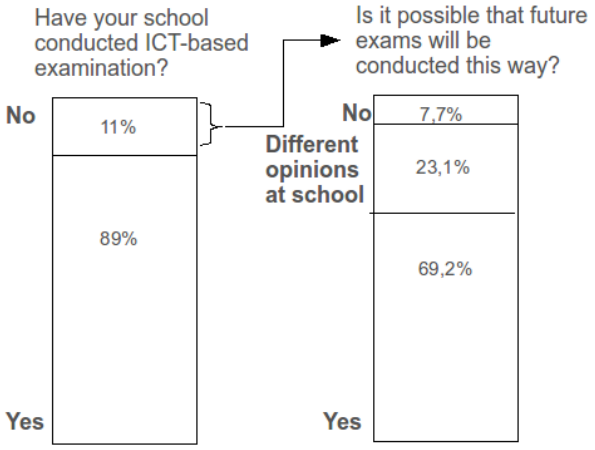


Figure 3: Question 1 & 5

Is it possible for the students to use their own computer in these examinations?

Further clarifications regarding what is meant with their own computer were given. Of the schools that had conducted ICT-based examinations, 48,5% answered that the students were allowed to use their own computer. The rest of the schools uses a combination of the schools stationary computers, and the schools laptops with prevalence of the latter with 32%.

Table 2: Question 4: Computer utilization

Yes	48,5%
No, only the schools stationary computers are used	19,4%
No, only the schools laptops are used	32,0%

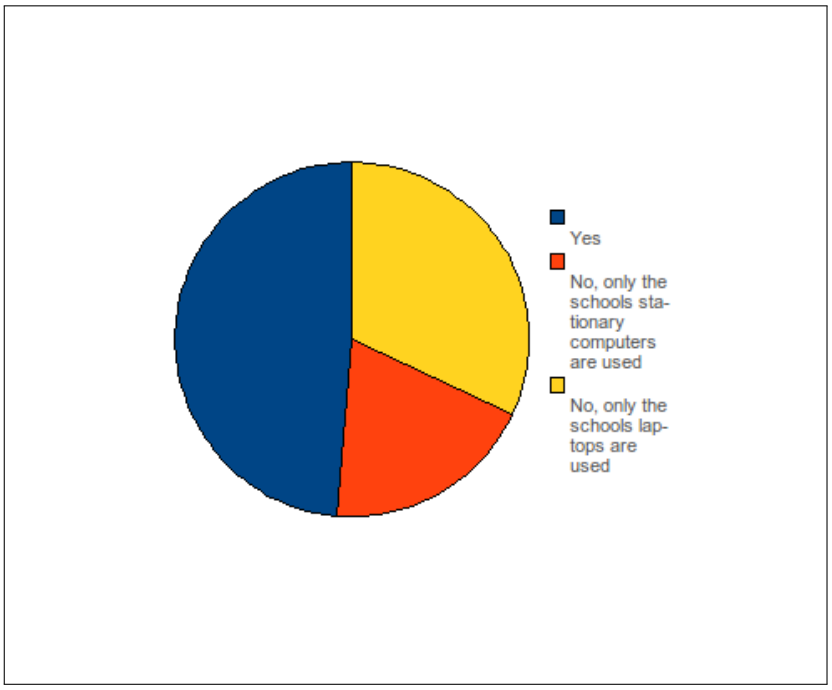


Figure 4: Question 4

If Internet or Intranet is necessary during the exam, how is this access provided?

Access is not provided at all in 7,8% of the schools asked, as they answered that "No exams is conducted with Internet/Intranet access". Most of these schools also answered "Yes" to the previous question about students using their own computer(5 out of 8). The majority answered that they were using a wireless network to provide this access with 67%, secondly wired access is used in 13,6% of the cases and the last "Other"-option got 11,7%. The majority of the "Other"-option was due to the fact that they used both wireless and wired access. In retrospect of the survey, a "Both"-option should have been included in this question.

Table 3: Question 6: Net access

Wireless	67,0%
Wired	13,6%
No exams is conducted with Internet/Intranet access	7,8%
Other	11,7%

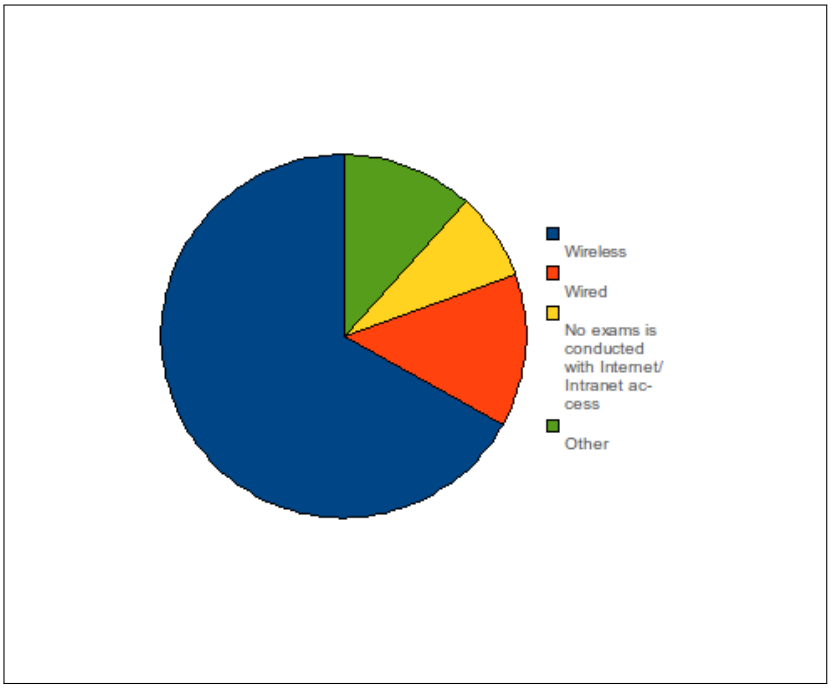


Figure 5: Question 6

How are the students identity verified?

With a slight majority of 36,3%, both traditional verification of identity and username with passwords are used. Secondly, 35,3% uses only username with passwords and 22,5% uses only traditional verification of identity. 5,9% answered "Other" in this question, some of these should have chosen one of the given alternatives based on the answers they provided.

Table 4: Question 7: Authentication

Both traditional verification of identity and username with password	36,3%
Username and password	35,3%
Traditional verification of identity is used	22,5%
Other	5,9%

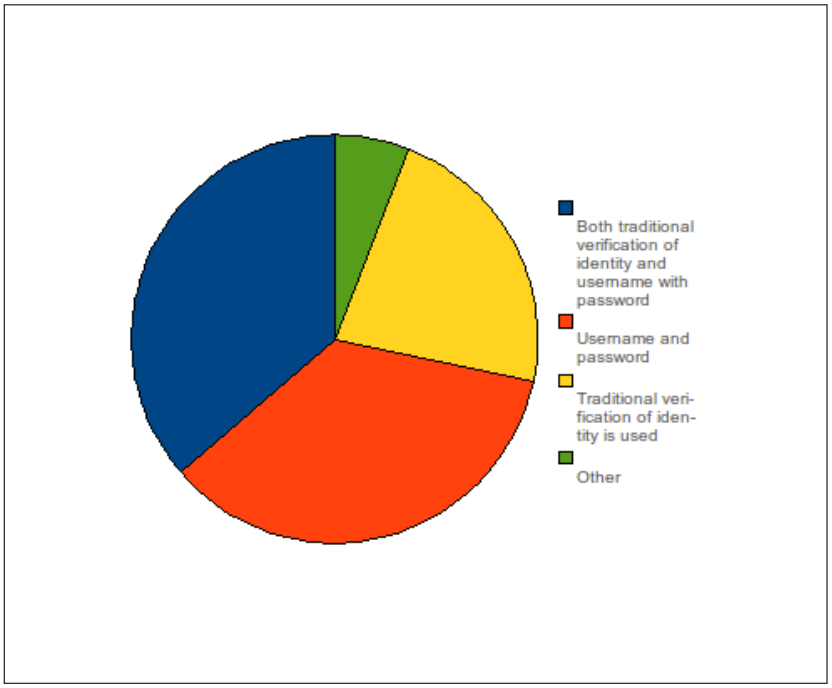


Figure 6: Question 7

How is the availability of the examination systems preserved during exams?

The majority of the respondents answered that they did not take any measures to assure the availability of the system. This majority accounted for 37,4%, some schools have redundant wireless access points (8,8%), others have some kind of other measure to ensure redundant Internet/Intranet access (25,5%). Redundant examination systems are used in 9,8% of the cases. Finally, 32,4% of the respondents chose to answer the "Other"-option in this question, but many of these have misunderstood the question and mistaken availability for access control[2]. Another reason for this misunderstanding might be poor definitions made clear to the respondents prior to the survey. This last part will be further reviewed in the discussion part of this report in Chapter 8.1.

Table 5: Question 8: Availability (multiple choice)

No measures are taken	37,4%
Several wireless access points are used to provide redundancy	8,8%
Other redundancy measure to ensure access to Internet/Intranet	22,5%
Redundant examination systems are used	9,8%
Other	9,8%

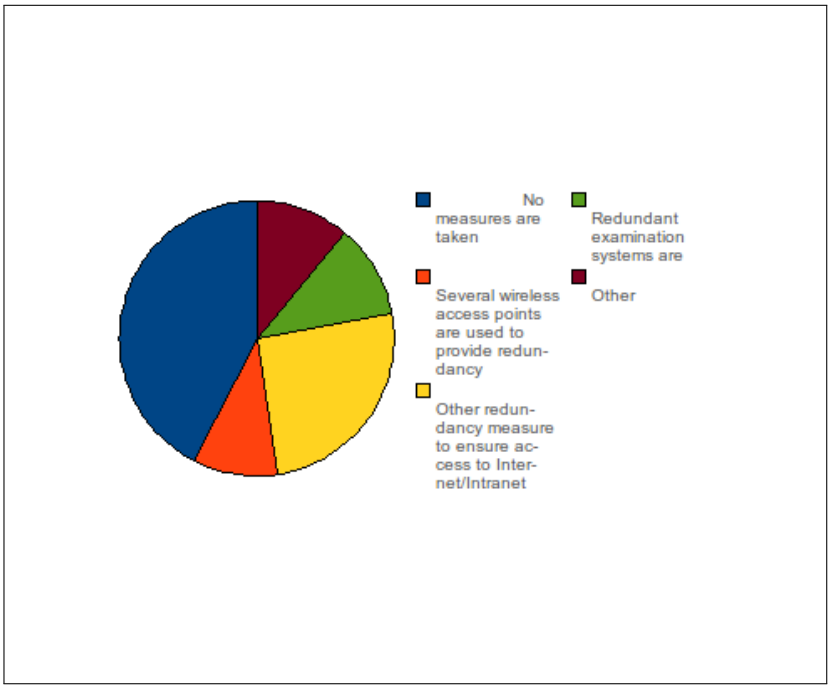


Figure 7: Question 8

[2]As this may sound strange, the Norwegian language opens for possible misinterpretations in this case, as the words "tilganger" and "tilgjengelighet" may cause some confusion

How is cheating mitigated?

The respondents were allowed to answer several of the answering options in this questions as they could all possibly apply. Most of the schools, 65%, are utilizing the invigilators to perform manual inspections to prevent cheating. 45,6% utilizes skilled personnel to do these inspections. Some of the schools, 32%, chose both of these options, which means that they utilizes a combination of these means to mitigate cheating.

Bluetooth communication and devices cannot be used in 41,7% of the schools as support for this technology is disabled. The same is true for external memory sticks or hard drives as 14,6% of the schools disables this support. 54,4% of the schools reports that they limit the net access to the schools Intranet. Finally, 34% had apparently more cheating mitigation implemented at their school as they filled out the "Other"-option too. Mitigation techniques to prevent ad-hoc wireless networks, surveillance and limiting use by using commercial software like 3ami-MAS[3] and BrowseControl are among the different elements mentioned here.

Table 6: Question 9: Cheating mitigation (multiple choice)

Manual inspection by invigilator	65,0%
Manual inspection by skilled personnel	45,6%
Bluetooth devices are disabled	41,7%
Support for external hard drive / memory stick is disabled	14,6%
Network access are limited to Intranet only	54,4%
Other	34,0%

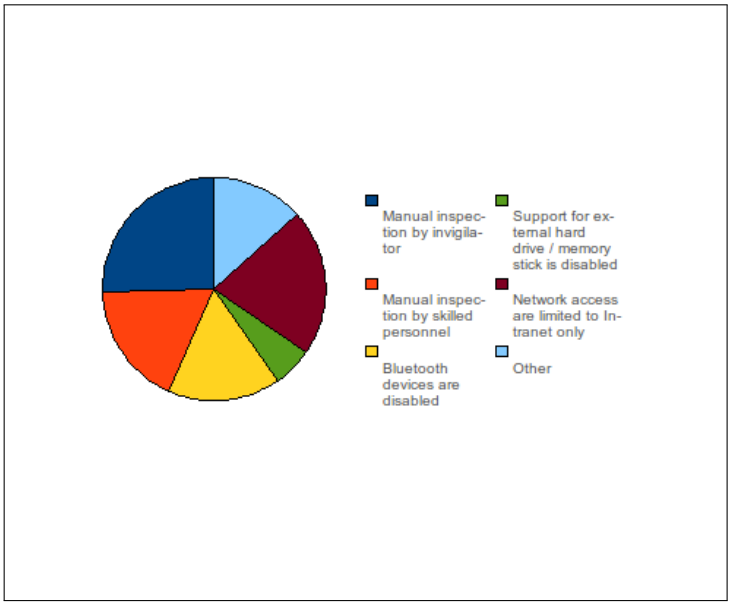


Figure 8: Question 9

[3]See this web page for case study from Norwegian high schools in the county of Nord-Trondelag: `http://www.3ami.com/latest-case-studies.htm`

How are document loss prevented regarding examination documents?

Document loss at the end of an exam may cause severe damage for students and prevention of this may or may not be implemented by the given examination system. In most cases, 71,8%, the student is responsible for regularly performing backups of their own work. Some of the schools, 18,4%, have implemented backup functions to handle this at a pre-set interval. Only 1% reports that they do not offer any prevention of document loss at examinations. 8,7% reports prevention of document loss in the "Other"-category. Some of these mentions that they can reconstruct most of the documents through the key logger used during the examination, others mention that they both encourage students to perform backups as well as automatic backups of the system.

Table 7: Question 10: Document loss prevention

The student is responsible to regularly save/backup document(s)	71,8%
The examination system regularly saves documents	18,4%
No measure for document loss prevention	1,0%
Other	8,7%

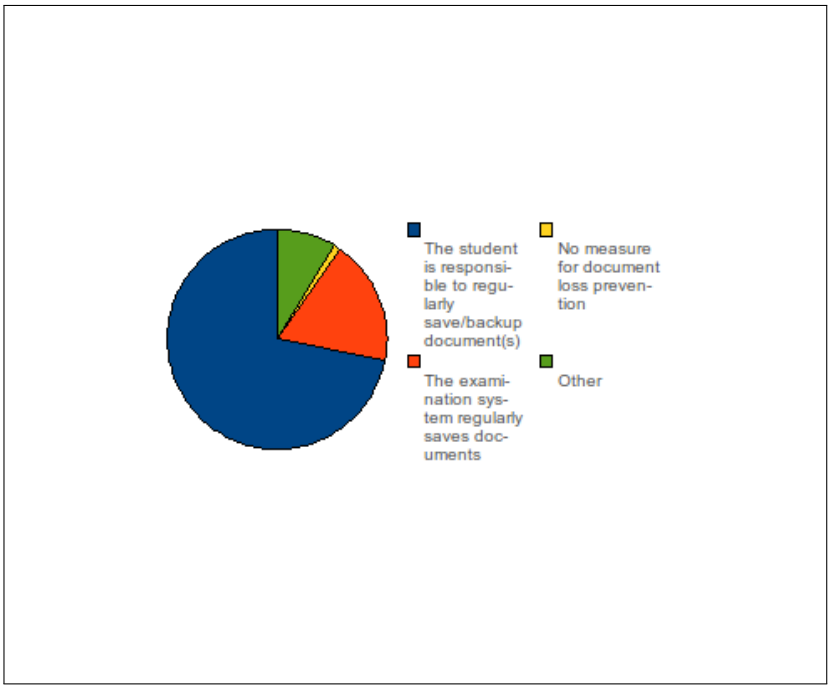


Figure 9: Question 10

What alternative methods for conducting an exam is used if the system goes down or in any other way is rendered unusable?

This question were included to discover what kind of contingency plans or strategies that are employed by the Norwegian high schools when conducting ICT-based examinations. It seems that most schools have employed plans of conducting the exam as a traditional exam if an unexpected situation would render the system unusable, as 64,1% answered this option. Notably less schools, with a 8,7% coverage, have a backup-examination system in place if the aforementioned situations occurs. Slightly more of the schools have actually no plans for these situations as 11,7% answers this alternative.

The "Other"-option is utilized by 15,5% of the respondents on this question. Some of the answers here should belong to the traditional[4] form of examination alternative. Others describes a situation where the students will finish the exam, but delivering it by printing it out on a local printer or by delivering the document on a USB memory stick.

Table 8: Question 11: Contingencies

Traditional examination is used instead	64,1%
Alternative examination system is used	8,7%
No measures to handle this situation	11,7%
Other	15,5%

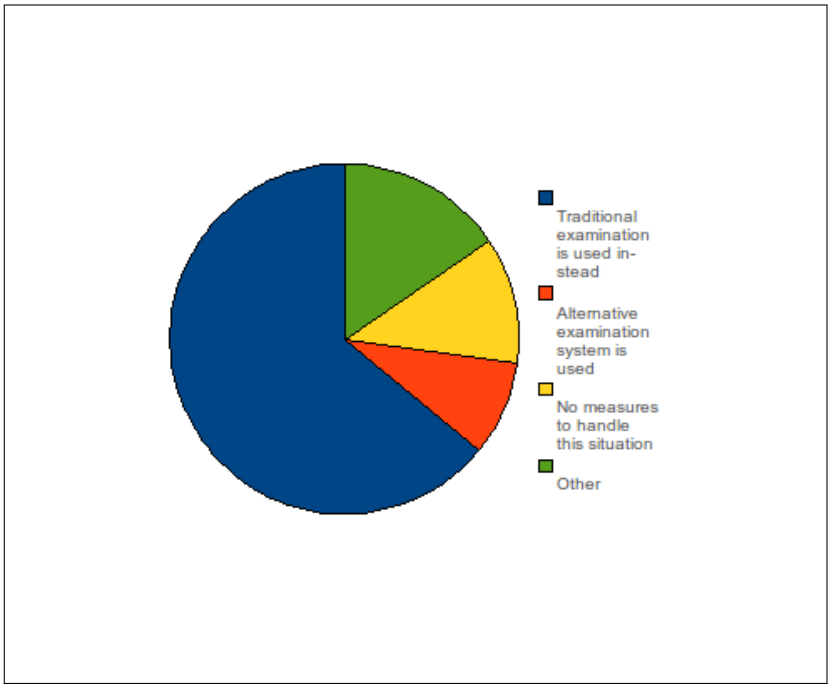


Figure 10: Question 11

[4]Pen and paper examination

How is confidentiality preserved with regards to exam questions and answers?

A little more than half of the schools in this survey have not implemented any measures to ensure confidentiality of questions and answers. About a quarter of the schools does however implement encryption to ensure this confidentiality. The rest of the respondents have chosen the "Other"-option and in this case many of them have responded that the responsibility of ensuring confidentiality is or should be handled by the PGS[5]-system provided by the Directorate of Education and Training.

Table 9: Question 13: Confidentiality

No measures taken	54,9%
Encryption is used	23,5%
Other	21,6%

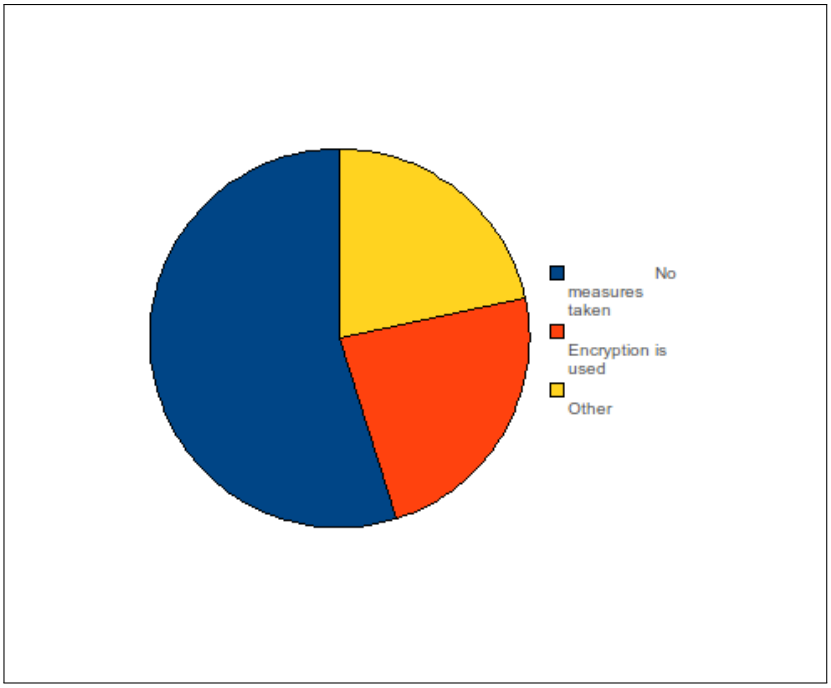


Figure 11: Question 13

[5]System for fetching and delivering exam papers

How is integrity preserved with regards to exam questions and answers?

Almost a third of the schools participating in the survey have not implemented any measure to ensure integrity of questions and answers. 5% of the schools are using digital signatures to ensure that integrity is preserved. The majority, 61%, believes that integrity is ensured with the access control that are implemented. 11% of the respondents chose the "Other"-option, and some of these are somewhat unclear about how integrity is preserved, and others relies on the PGS to ensure this.

Table 10: Question 14: Integrity (multiple choice)

No measures taken	30,0%
Digital signatures are used	5,0%
Ensured with access to authorized personnel only	61,0%
Other	11,0%

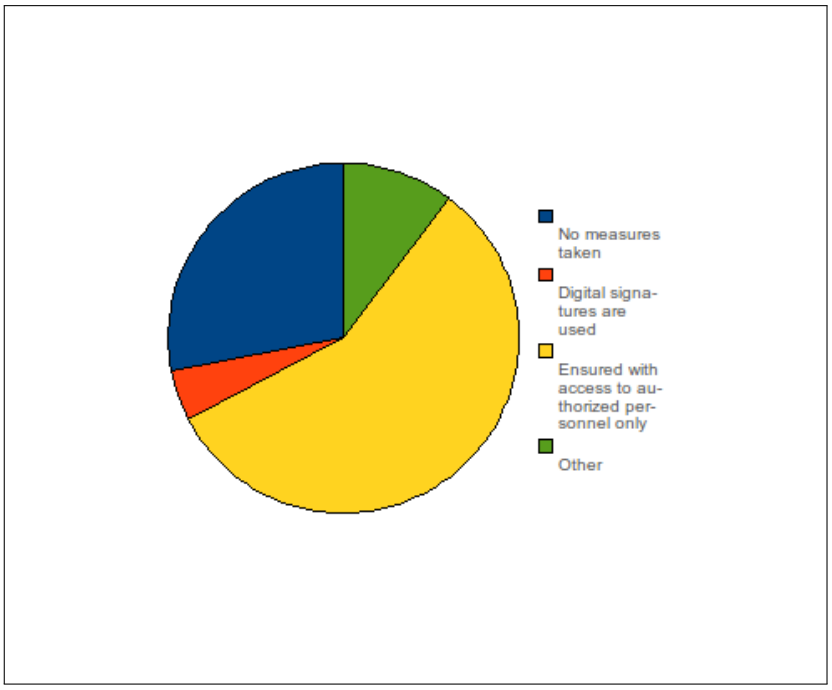


Figure 12: Question 14

How many cases of cheating have been discovered per year?

The majority of the schools that responded have not experienced any form of cheating, while 24,2% reported 1 to 3 cheating incidents per year. 4% reports 4 to 6 incidents, and finally 2% have experienced cheating in 10 or more cases per year.

Table 11: Question 15: Cheating incidents per year

None	69,7%
1 - 3	24,2%
4 - 6	4,0%
7 - 9	0,0%
10 or more	2,0%

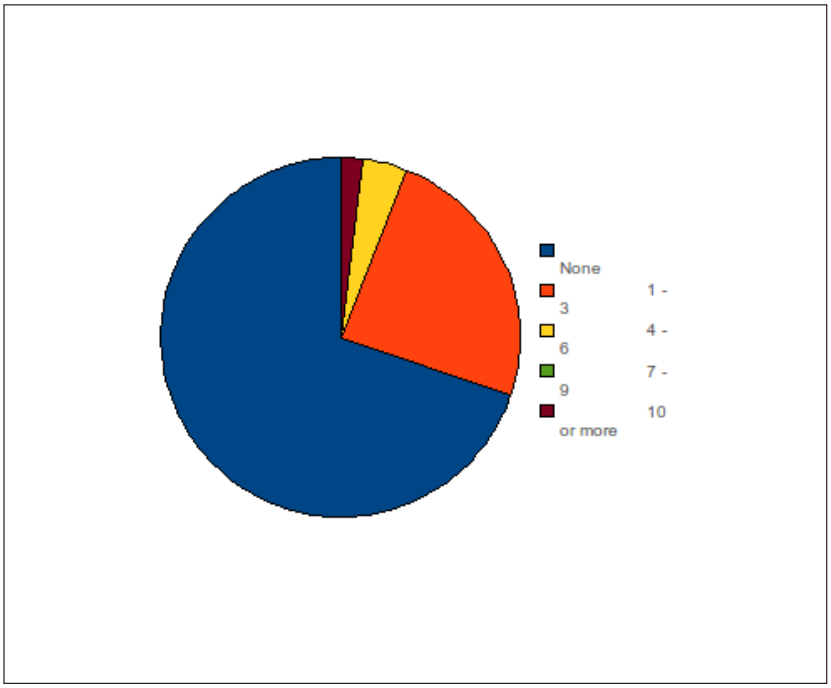


Figure 13: Question 15

This means roughly 90 cheating incidents per year, and if we assume that each new incident is caused by a different student, then 1 in 486 students have cheated in the last year. These incidents are the ones that are detected and reported, it would be useful to look into the possibility of dark figures in this matter. More on this issue in Section 8.1.

The schools that reported incidents of cheating were asked how this was conducted. A lot of different reasons and methods were explained, and the following list covers these:

- BrowseControl have unexpectedly stopped working or students have found ways to circumvent this tool to gain open Internet access
- Copy+Paste from Internet or other sources have been detected

- Communication with other people, e.g. with a cell phone
- Folder sharing on local network
- Misuse of communication over Internet
- Students have hooked up with near-by wireless networks to bypass security restrictions on the given network
- IP-addresses that should have been blocked were not, due to typing errors. Made it possible for students to access open Internet.
- Illegal use of dictionaries or translation applications
- Students have gained administrator access
- Students have copied papers from their own computer
- Students have exchanged examination usernames and passwords

How is unwanted communication prevented among the examination candidates?

About half of the schools that responded in this survey is limiting the network access with a firewall to reduce the possibilities for communication with the outside. Similar communication is prevented in 27,5% of the schools by using a dedicated application to filter URLs based on a rule set, while 21,6% of the schools reports that they prevent this communication with prohibition of network access. Use of unauthorised wireless networks are blocked or prevented in 32,4% of the cases and bluetooth is prohibited in 39,2%. Similar limitations are enforced regarding mobile broadband where 27,5% prohibits this. About 20% of the schools have more measures to mitigate unwanted communication as they have answered the "Other"-option. Some of these schools uses proprietary software to monitor or control the candidates. Other schools implement measures such as keyloggers to capture every event from the keyboard, radio direction finders or magnetic field meters to eliminate rogue access points, surveillance and logging of events triggered by the candidate and two schools have used digeks to mitigate illegal communication.

Table 12: Question 17: Communication prevention (multiple choice)

Limited network access with firewall	52,0%
Limited network access with dedicated filter application (WebSense etc.)	27,5%
No network access	21,6%
Use of bluetooth is prohibited	39,2%
Use of unauthorised wireless networks are blocked	32,4%
Use of mobile broadband is prohibited	27,5%
Other	19,6%

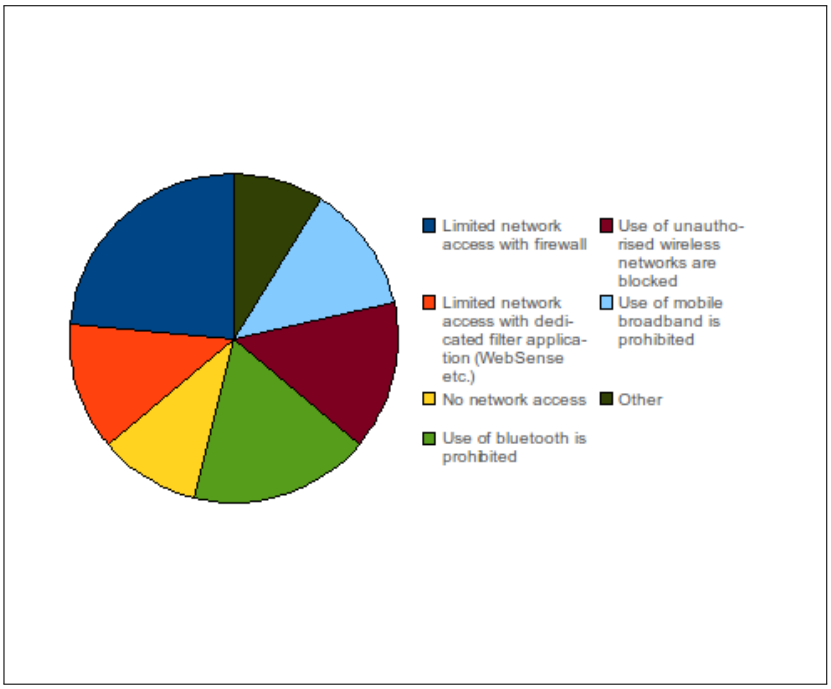


Figure 14: Question 17

How is non-repudiation preserved in the examination setting?

About half of the respondents chose to not answer this question. Some of the reason for this might be that this question had an open text answer while many of the others have been multiple or single alternative questions. Another reason might be that the respondents were a bit unsure about how this is ensured. Some of them explained that this is handled by the PGS system, and others answered that they did not know or that this question should have been directed to person responsible for administrating examinations. Other respondents describes a solution where students prints a receipt for the exam which they signs and deliver.

Which local applications are accessible for the student during the exam?

Half of the schools allows all applications during the exam, while about 20% disallows translation applications and all other is permitted. 23,3% is slightly more strict as they enforce a policy that disallows all applications except for the ones necessary to carry out the examination. Most of the 4,9% that chose the "Other"-option seems to fit into the strictest of the aforementioned alternatives. Additionally, one school disallows alternative web browsers, presumably as their monitoring or filtering software will not function with other browsers.

Table 13: Question 19: Application access

All applications	52,4%
All applications except translation applications in foreign language courses	19,4 %
Only necessary applications to carry out the exam	23,3%
Other	4,9%

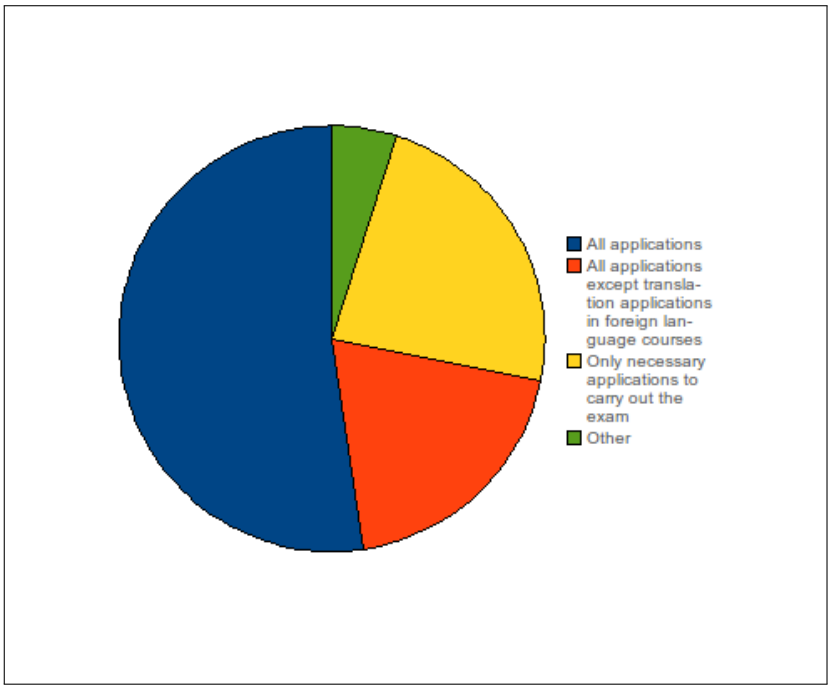


Figure 15: Question 19

What are the security challenges that is handled poorly with today's system?

Many of the schools have difficulties with the technical competence gap between invigilators and students, and lack of control due to this is the most widespread security challenge as almost 70% of the schools have difficulties regarding this. The second most widespread challenge is to block illegal communication, which over 60% of the schools have problems with. Difficulties regarding blocing illegal resources, both external and internal, is of somewhat less concern as around 30% of the schools struggles with this.

Some of the respondents who chose the "Other"-option proclaims that the form of examination used today is not suited to be used in ICT-based settings. IR-communication is also mentioned as a security challenge. Some other respondents uses this option to explain that they feel they have good control by using "digeks" or "3ami-MAS", not to be confused as the latter is more dedicated to surveillance of computer system and the former is the ICT-based examination system with an administrator module which invigilators can see if the students are connected to the system or not.

Other security problems that is mentioned here are availability regarding the PGS-system as it has had some problems with a large number of multiple and simultaneous login attempts.

Table 14: Question 20: Security challenges (multiple choice)

Difficult to control due to unskilled personnel during the exam	68,8%
Difficult to block communication	61,5%
Difficult to block access to external resources	35,4%
Difficult to block access to local resources	31,3%
Other	18,8%

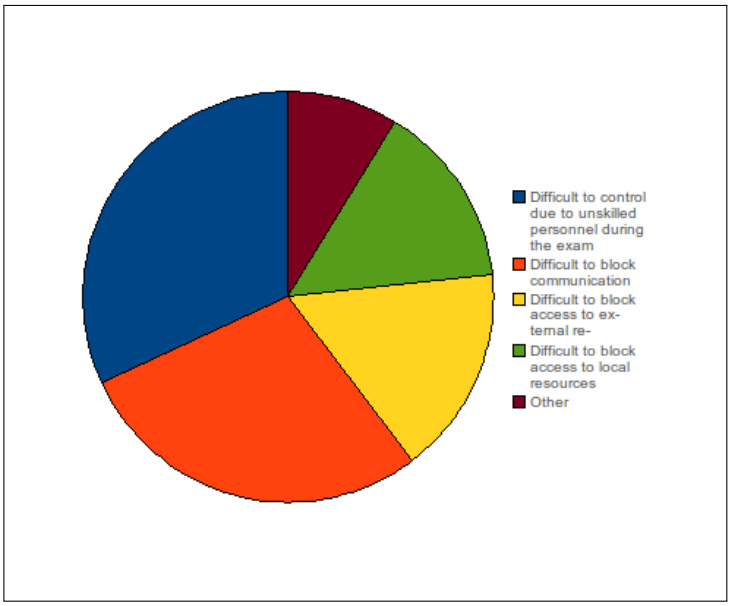


Figure 16: Question 20

How much are the students being kept under surveillance during the exam?

We asked this question to get a rough estimate regarding the degree of surveillance the students are kept under. No surveillance is used at all in 13,6% of the schools, while 43,7% has implemented some monitoring of activity. Almost a third of the respondents answers that they perform surveillance at a medium degree. The last 12,6% is admitting that they keep the student under surveillance at a high degree where more or less all activity are monitored.

Table 15: Question 21: Surveillance

No surveillance	13,6%
In some degree (some monitoring of activity)	43,7%
In medium degree	30,1%
In high degree (more or less all activity are monitored)	12,6%

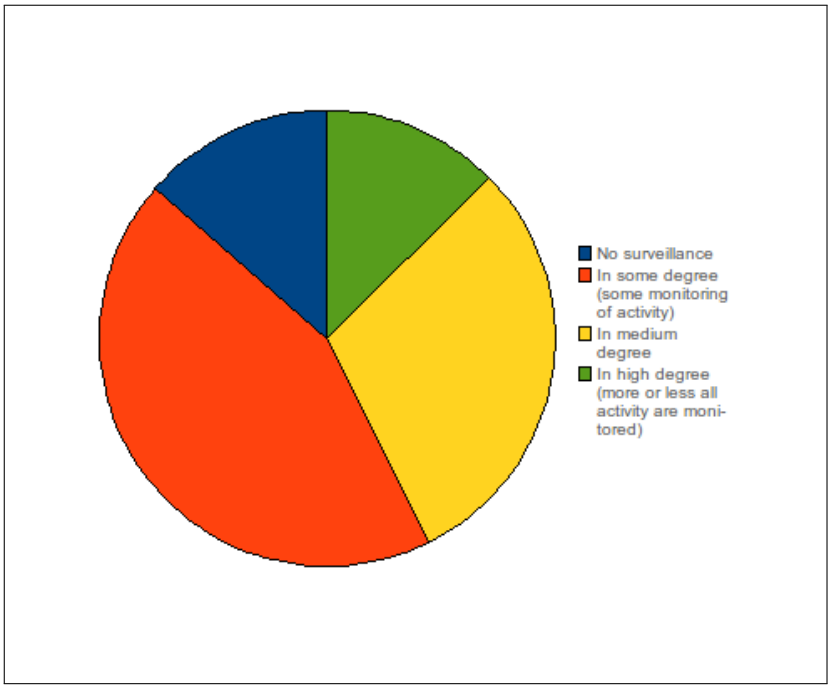


Figure 17: Question 21

3.3 Association

In order to analyse the data, some relationships between groups and variables is desirable to investigate. We wanted to examine the effect of allowing the students to use their own computer. For this analysis we have regrouped the three groups in question 4 to contain two groups where the first group allows student computers and group two allows only school controlled computers. Hereby refered to as Group 1 and Group 2 respectively as shown in Table 16.

Table 16: Regrouping computer utilization

Group 1	**Group 2**
Student computer is used	School controlled computer is used
48,5%	51,5%

If we compare these two groups against the method of connectivity for Internet we see the tendency that schools who allows student computers are more inclined to use wireless access. Only 7% of the schools which allows some form of Internet connection in group 1 uses wired network compared to the 27,5% within group 2, this is also illustrated in Table 17. The results shows that this relationship is in fact statistical significant, with a significance level of 0.013 based on the Chi square test.

Table 17: Computer utilization and network access

	Student computer	**School computer**
Wireless	93,0%	72,5%
Wired	7,0%	27,5%

However, statistical significance is not found when the groups are compared to application policy. In fact, there seem to be no tendency to be such association either as the observed values are almost spot on compared to the expected values. This means that schools does not allow or disallow certain applications based on what computer the students are using.

Possible association between the use of own computer and the degree of surveillance were also examined. A t-test was used for this purpose based on the distribution of the surveillance degree data set. The results shows that it is a slight tendency of more surveillance when the school controlled computers are used, but it is not enough difference to be statistical significant.

We wanted to see if there were a significant difference in the amount of security challenges between the groups. An index which sums up the amount of security challenges for each school were used and the results shows a difference between the groups but the t-test performed shows that the result is not statistically significant.

We also wanted to see if there were a significant difference in the amount of security measures between these groups. An index were made here also to sum up the amount of measures. Some tendencies were also observed here but again no clear statistical significance. The tendency were regarding more implemented measures for the school controlled computers. Blocking of bluetooth access and external memory devices were the measures with highest level of significance, i.e. the blocking of bluetooth had a significance level of 0.051 which is close to the 95% threshold and the blocking of memory devices resulted in an asymptomatic significance of 0.067.

Another hypothesis was that by using the school controlled computers, more incidents are reported. The t-test shows that it is a clear tendency of this behaviour, but it is not statistically significant (0.055). Additional filtering on schools that allows Internet access, shows that this association reaches the threshold of 95%. This means that it is a 95% chance that this statement is true: "High schools that uses school controlled computers with Internet connection during ICT-based exam are more inclined to report cheating incidents as opposed to schools that allows student computers in the same setting".

An other way to detail the incidents in the different groups was to regroup the cheating incidents group to either reported or not reported incidents. The results shows that only 17% of the schools in group 1 have reported cheating incidents whereas 43% of the schools in group 2 have done the same. These results are also significant as the significance level is as low as 0.005.

3.3.1 Survey summary

Nine out of ten schools have already condcuted ICT-based examinations. Only one of the schools reported that they have not and will not perform these examinations. This particular school is a culture based school which teaches music, dance and drama courses at the high school level on behalf of another high school.

Over half of the schools permit all application during the examination on the computers. This means that even if network access is blocked, the student might use a pre-installed program to cheat on the exam. Additional 19% of the schools employs some form of blacklisting by disallowing translation applications in foreign language examinations. We can only assume here, but a complete list of translation applications to fill this blacklist would be extremely difficult to gather and this list would have to be updated at a fairly regular basis to cover all illegal applications.

Approximately 2 in a thousand has cheated on the exam according to reported incidents. This number seems low, but when compared to a survey [27] in a Norwegian University which concludes that about 90% of the cheaters are never caught, it could possibly mean that about 20 in a thousand have cheated on the exam. Some properties of these two populations may have shifted from the high school environment to the college environment, and it would have been an interesting experience to examine the dark figures on this matter.

The degree in which the schools reports that they perform surveillance of their students varies from none to a high degree. An assumption of proportional increase in reported incidents based on the level of surveillance, were made prior of the survey results. However, according to the results, the number of incidents decreases from the "Some degree"-group to the "Medium degree"-group. See Figure 18 for an illustration.

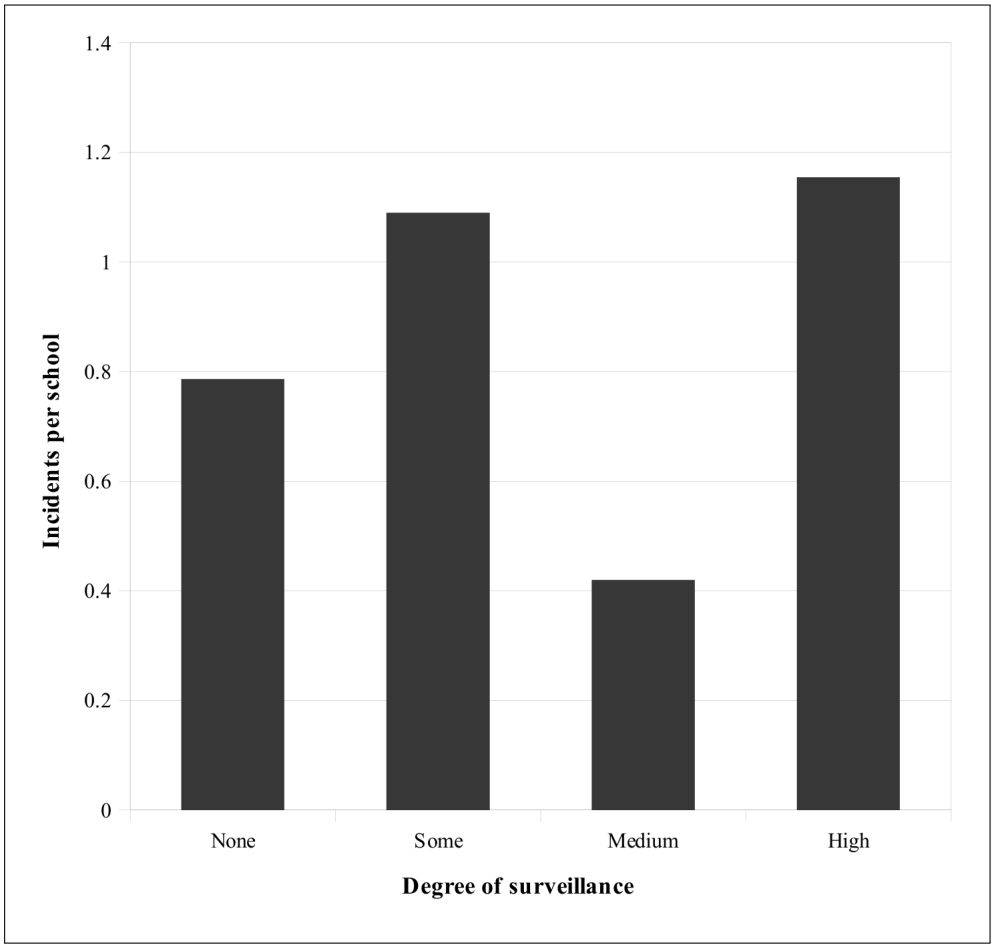


Figure 18: Surveillance degree and incidents

This observation indicates that the increased level of surveillance does not necessary mean that more students is caught cheating. The incidents per school is found by using the total number of incidents in a group and the size of that group. The actual numbers can be found in Table 18.

Table 18: Surveillance and incidents

Degree of surveillance	None	Some	Medium	High
Group size	14	45	31	13
Incidents	11	49	13	15
Incidents per school	0.79	1.09	0.42	1.15

The observed outcome of this analysis shows a significant deviation from the expected outcome and the significance level were calculated to be 0.227.

One more observation to emphasize is the role of the invigilator in the examination scenario. At one side, the invigilator is the most used measure to prevent cheating. At the same time, invigilators are seen as part of the most common security challenges due to their lack of necessary technical skills. When comparing the groups that are worried about using invigilators and the

groups that uses invigilators as a security measure the tendency shows that the group that is worried is also more inclined to use invigilators as a security measure.

We have also seen that schools that prefer to use their own equipment on an Internet enabled exam, is more inclined to report incidents than schools that permit students to bring their own computer.

4 Background and theory

In the following chapter some background information about how ICT-based examinations are conducted today will be reviewed. Both procedural and functional aspects of the examinations will be discussed. Terms in the matter will be defined and assumptions will be clarified. Relevant theory will also be discussed.

4.1 Background and prerequisites

To be able to create a solid security framework for ICT-based examination systems, background information about the environment in which the framework will be implemented must be known. Some of the background information has been gathered in the survey sent out to the schools. We have extracted that a good amount of schools allows the students to use their own computer at the examination and over half of the schools uses a wireless configuration. A typical network structure based on the answers from the schools can be seen as a rough illustration in Figure 19.

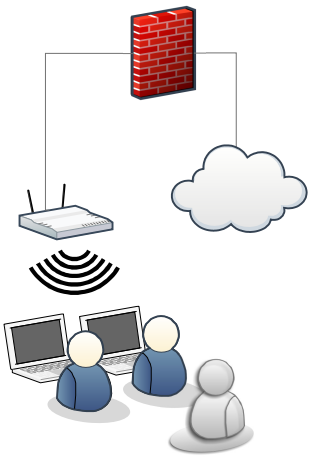


Figure 19: Rough network layout

4.1.1 Procedural and functional requirements

There were 446 high schools in Norway during last school year with a total of 183.802 students [28]. The existing procedural and functional requirements in Norwegian high schools is relevant for this thesis as the framework will be developed with this environment in mind. The schools are instructed to use only Internet for purposes such as fetching and delivering of the exam. How this is controlled is up to each school, but there are some guidelines [29] about which IPs should be allowed and requests to other IPs should be blocked by the firewall at the different schools.

Examination procedure and roles

One person at the different schools has the responsibility for the examination, and this person is further refered to as the examination administrator. For the centrally given examinations, these are the general instructions [30] for how the exam is conducted:

- The examination administrator fetches user names and passwords for the given exam
- The credentials are distributed to the examination candidates
- At the start of the exam, these credentials are used by the students to log in
- The log in process is not complete until the examination administrator verifies the ID of the candidate and (or his/hers representative) provides an additional password unique for the given exam.
- The candidate can now download the examination paper(s)
- The answer is uploaded to the system at the end of the exam, alternatively the answer is delivered by paper printout

While the examination is conducted it is under the supervision of one or more *invigilators*, and in some cases these are instructed to inspect the students and their screens [31]. Some roles in this scenario can be depicted based on this information. First of all, the student which acts as an examination *candidate*. Secondly, the *examination administrator* which acts as a manager and verifier of identities. Lastly we have the invigilators which supervises the candidates while they conduct the exam.

Examination model and allowed aids

There are some guidelines [32] on what kind of aids are allowed based on the examination model. Two main models are used for this purpose. Model 1 is the ordinary exam where all aids are allowed, except access to Internet and other tools that enables communication. An exception to this rule exists in examinations for language subjects where translation applications are disallowed. Model 2 is a divided exam containing one part where only writing materials, compasses, ruler and protractor is allowed. Second part is similar to model 1 where all aids are allowed.

4.1.2 Definitions and assumptions

In order to confront some of the issues related to ICT-based examinations and information security, some definitions have to be made clear a priori.

Illegal assistance:

is the assistance that an examination candidate receives from a person that is not authorized to give such assistance.

Illegal aids:

is information or resources used by the candidate from illegal sources. The different examination models determine which aids are allowed.

Cheating:

is when a candidate either takes use of illegal aids or illegal assistance during the examination.

Internal drive resources:

is information or applications existing on the computer hard drive a priori of the exam.

External drive resources:

is information or applications located on removable media attachable to the computer used for examination.

Network resources:

is information or applications located on remote network connected hosts or servers. These network resources can be used as part of communication used in an illegal assistance setting.

Traditional identity verification:

is authentication of students with use of physical ID for verification.

4.2 Relevant theory

The subject of this thesis covers multiple areas of the information security field. First of all, it is both a theoretical and practical take on information security and it covers different aspects of security engineering. Ross Anderson proclaims in [33] that good security engineering consists of policy, mechanism, assurance and incentive. The three first elements he mentions here will be a returning topic of this thesis. Incentive however, will not be reviewed in detail here and exploring this will be a part of future work.

4.2.1 Security of the design

An important aspect to the security of any system being developed is the security of the design. This should be an important part to remember here as well, and the essence of good security design are represented by the design principles of Saltzer and Schröder[34]. We will briefly present these principles and their relation to different parts of examination systems.

Economy of mechanism - hardening the host

The key aspect of this design principle is that complex systems is harder to protect than less complex systems. Another term that is used to describe this principle is Keep It Simple Stupid (KISS), and it is thereby desired to harden the host or system as much as possible without loosing key functionality.

The examination systems covered by this thesis can be described as limited purpose systems, as opposed to regular desktop operating systems which normally intends to be multiple purpose systems. Due to this property, limiting the usage of unnecessary applications and services is a key factor to decrease the attack surface. Host hardening is mostly used to describe systems that limit the usage of applications and services to be accessed from the outside. In this case it is extended to include accessing these applications and services from the inside as well.

Principle of least privilege

The essence of the principle is that entities should operate using the least privileges needed to complete a given operation. There is no need for the student user to have permission to do a lot of configuring in the system settings as an example in the exam scenario.

Open design

The object of this principle is to avoid security by obscurity. This is also applied in cryptography, where there are assumptions that the adversary knows what encryption algorithm is used. This should also be the case of examination systems, security measures should not rely fully on secrecy.

Fail-safe defaults

The principle advocates that actions should be default denied wherever possible. This means that if an action is not explicitly allowed, there should exists a mechanism that blocks the action.

Complete mediation

The essence of the principle is that every access to every object must be checked for authorization, and every subject must be identified. A reference monitor in an operating system has this purpose, and should also be a part of the operating system / examination systems used in the exam scenario.

Separation of privilege

The concept is that for certain actions, forced cooperation in asserting privilege is needed. A real life example on this security measure is safety deposit boxes in banks where a bank clerk or manager has one key and the customer has the other. The box cannot open without the cooperation of both parties. Critical functions in an examination system could also adopt the concept of this principle.

Least common mechanism

Proclaiming limited use of shared mechanisms that can perform as an information flow conduit, the principle is often connected to the mitigation of covert storage channels [35]. In the exam scenario we would like to keep the shared mechanisms between students and persons outside the examination room at a minimum to prevent leakage of information.

Psychological acceptability

The complexity of security mechanisms should be at a manageable level. There are several examples [36] of cases where security measures that is hard to live by is bypassed in order to complete a certain task. The principle acknowledges that the human factor is a big part of security and should not be underestimated. It is important to develop security mechanisms that match the mental image of what this mechanism is supposed to do.

4.2.2 Security measurement of systems

A lot of work has been done in the process of finding good security metrics to measure the security level of a given system. We are not going very much in depth here, but some methods and principles in this matter will be mentioned.

In his paper on computer security [37], Landwehr argues that the assurance that a system functions properly relies on three different sets of evidence. First it is the evidence that the system or device has been developed by motivated personnel with a high skill level. Secondly it is the evidence that the system or device has been developed with a secure process that ensures the fulfilment of specification intended for the device. The last evidence lies in the testing and

analysing of the product directly. He further argues that this last evidence is the strongest as it does not matter who built or what process was followed if it performs as intended. This master thesis will mainly focus on this evidence in order to establish assurance in the examination systems that will be investigated.

Murdoch refers to the evidence described by Landwehr when talking about trust and assurance in the paper [38] concerning security measurement. He also states that there exists two related levels of trusts involved in this setting:

> in the system and in claims about the system; both have to be addressed.

Our intention is to follow this philosophy by first investigating claims regarding implemented security measures, followed by testing of these measures to see if they perform as intended.

Threat analysis

In order to achieve a solid measurement of the level of security a system yields, some foundation must exists and a threat analysis is an important part of this analysis. The importance of a threat analysis is emphasized in [39].

Threat agents

The first element to investigate here is who the threat agents are. From a simple view, the threat agents in this scenario is mainly students with the intent to cheat on an exam or to postpone the exam, hereby also referred to as internal threat agent. An extended perspective on threat agents could include students or other persons looking for an opportunity to invalidate another students examination answers, hereby also referred to as external threat agent.

When modeling threat agents in the process of assessing the security of a system, Murdoch et al. describes in [38] how examples with terrorist threat agents could be used. The example was originally modeled by Jones et al. in [40] and gives some factors on how a threat agent can be classified:

- Group size
- Level of education
- Cultural factors
- Access to communications and the Internet
- Technical expertise
- History of activity
- Sponsoring countries
- Funding

Without trying to compare terrorists and students, some of these aspects can be transferred to the student domain. The least relevant factors is the cultural, sponsoring countries and the activity history factors and will be dismissed for the purpose of this master thesis.

When it comes to group size, a safe assumption would be that the group would be rather small and in most cases consist of only one person. In the case of external threat this group size might increase some more but with no more than 5 persons. The level of education will in most

cases be somewhere situated in the high school level, and the technical expertise might in some cases reach an intermediate level. Access to communications and the Internet will be high in the case of external threats, but it will be low in the case of the internal threat as a result of what communications means are allowed during the examination. Funding will in most cases be limited, but one would also have to assume that some of the students have access to more funds than others. The threat agents for both external and internal threats are summed up in Table 19.

Table 19: Threat agents

	Internal	**External**
Group size	Small (1-2)	Small (1-5)
Level of education	High school level	High school level
Technical expertise	Intermediate level	Intermediate level
Access to communications and Internet	Limited access	High access
Funding	Limited to medium	Limited to medium

These numbers and levels are no more than an educated guess and we should for example not underestimate the possible technical expertise of students or other threat agents. However, with this threat overview, we can include this factor when assessing and testing ICT-based examination systems.

5 Analysis of current solutions

In this chapter, we will initially perform an assessment of the systems we later intend to test. There exists methods that have been developed for this purpose. One of these were discussed in section 2.1, and with some modifications will be used to gather information about the theoretical security level of the system to be further investigated. The full set of assessment items will be sent to the respective systems key personnel as a self assessment form. When returned, the security of the system will be assessed and their answers will form a basis for what elements will be included in the testing phase. A scale will be developed with the purpose of rating how well the security measures perform according to their goal.

Two ICT-based examination systems are chosen to be part of the assessment and testing in this thesis, namely digeks and eExam. These were briefly explained in Chapter 2 where we saw that they allowed the students to use their own computer. Additionally, both are based on open source operating system and are freely available for the public on their respective project pages [17, 41]. For the testing phase, default installations of these systems will be used. More information regarding the testing phase will be given after security assessment of digeks and eExam.

5.1 Assessment of theoretical security

The values of the different security services in the assessment framework presented in the work of Eibl et. al [7] will be used as a basis for the assessment phase here. The framework is intended for use when assessing security in an e-learning environment, but in addition to the identified security services, categories of non-repudiation and authorization and their respective security services will for the purpose of this assessment be added to the adapted assessment framework. These services will be appointed their own levels of security based on an evaluation. This evaluation will be conducted from Section 5.1.1 to Section 5.1.8 and will be our contribution to this framework. The final framework that will be used for the assessment will be presented in Section 5.1.9. As well as new services in new categories, some of the already established security categories will include some new services that will complement to the security of an examination environment.

5.1.1 Non-repudiation services

These services provide non-repudiation; gains confidence that the student who delivered an exam answer cannot deny of having done so. This can be performed by the means of digital signatures or one time password tokens. As the examination system can be a part in a bigger system, non-repudiation can be provided by external systems or services. Trusting these external and maybe somewhat unknown security measures yields a lower score than measures implemented in the assessed system.

ID	Weight	Description
2.1	[0.7]	Ensured with digital signatures
2.2	[0.6]	Ensured with OTP token
2.3	[0.2]	Ensured by external system

5.1.2 Integrity services

It is of considerable importance that the system/operating system cannot be modified or replaced in order to aid the candidates to cheat. I.e. the integrity of the system must be preserved, and service 3.5 focuses on this point. As another security service, intrusion detection can be used as a method in preserving this integrity through accountability and proper response to incidents. Building the system with measures that protects the integrity of the system is somewhat more proactive than the intrusion response method of preserving this property and thus gets a slightly higher score.

ID	Weight	Description
3.5	[0.7]	Operating system integrity is preserved
3.6	[0.5]	Intrusion detection mechanism implemented in system to detect privilege escalation or other malicious activity

5.1.3 Encryption services

The assessment framework already includes encryption of information in transit, which undoubtedly is the most important encryption service. To complement this, we have included a service that handles stored content in regards to encryption as well. As the availability and stealthiness of an eavesdrop attack might be somewhat higher than with an attack involving stealing the USB flash memory stick unnoticed, the newly added encryption service also gets a lower score.

ID	Weight	Description
4.3	[0.6]	Encryption of stored exam content

5.1.4 Services to disable network communication

These services will prohibit illegal network communication to prevent the candidates from exchanging messages with each other and with external parties. Restrictions provided by the examination system itself together with some firewall is covered by these services. A firewall that is coupled with the access point the examination students are supposed to use is all well and fine, but if there exists rogue access points or the possibility to enable such elements, that firewall won't matter and mitigation against rogue access points should be taken. Security services that include Bluetooth and infrared technologies are included in this scheme as well as these can enable illegal communication. The effort made for an attacker to connect to networks through Bluetooth or rogue access point should be considered as slightly higher than just connecting to the regular network available. For this reason, these services are rated somewhat lower than security services that prevent network communication either in the system or in the infrastructure with the use of a firewall.

ID	Weight	Description
5.1	[0.7]	Access to Internet is restricted/limited by examination system
5.2	[0.6]	Access with Bluetooth/IR to other devices or networks are completely disabled
5.3	[0.7]	Access to Internet is restricted/limited with a firewall
5.4	[0.6]	Access to rogue access points are prohibited

5.1.5 Prohibiting illegal access to hard drives

Hard drives, both external and internal, may contain information that can be considered as illegal aids in the context of an examination. Tiny and cheap USB memory sticks can contain an enormous amount of data. For these reasons, it is important to prohibit access to these devices. The advantage of access to own internal hard drive for a cheating student may be compared to that of communicating freely over the Internet, as the student may have mirrored relevant sites, documents and tools to his or her own computer. For this reason, the weight will be the same as for the Internet-restrictions, but a little less for the prohibition of external hard drives as these will yield less stealth. The mentioned weights can be seen in Table 5.1.5

ID	Weight	Description
5.5	[0.7]	Access to internal hard drive is prohibited
5.6	[0.6]	Access to external hard drives are prohibited

5.1.6 Secure failing service

In order to adhere to the security policy the system must not be susceptible to attacks which is engaged by enforcing a crash of the system. This might lead to unauthorized privilege escalation, and mitigation techniques to ensure that the system fails gracefully and with authorizations that should be in place. It is important to prevent this and service 5.7 is used for this purpose. This service is rated lower than for example 5.5 and 5.6 because of the assumption that the skill set needed to carry out an actual privilege escalation attack is higher than attacks towards those services.

ID	Weight	Description
5.7	[0.5]	Security mechanisms of system cannot be circumvented by crash

5.1.7 Security services to mitigate running system in a virtual machine

The security policy of a given examination system can be circumvented if there are possibilities to run the system in a virtual machine. This is at least true for the systems which uses live version of an operating system, such as digeks and eExam. Services 5.8 and subservices 5.8.1 and 5.8.2 covers these problems. While 5.8.1. covers the technical mitigation of running the system virtually, 5.8.2. provides only procedural methods to confront the problem. Procedural techniques are by no means unimportant, but as this assessment focuses on the technical side of security for examinations, the rating is better for a system with technical countermeasures.

ID	Weight	Description
5.8	[0.6]	Security mechanisms of system cannot be circumvented by running the system in a virtual machine
5.8.1	[0.5]	Secured by implementing technical security measures to prevent circumvention
5.8.2	[0.4]	Secured by implementing procedural security measures to prevent circumvention

5.1.8 Separation of privilege service

The service is labelled ”6.7 Exam content only accessible with dual authentication (one for student and one for invigilator/system administrator)” and it is referring to the principle of separation of privilege and is an important part of the design principles of Saltzer and Schröder in [34]. The essence of the principle is that it is more secure to use two different keys instead of just one to access a object. In a real life scenario with examination of students, the invigilator with the second key will know that the exam candidates that are enrolled in the system have, with great confidence, been verified to be in the supervised and intended room for the exam period. The invigilator can also use this service in the process of verifying the identity of the candidates, i.e. only candidates with valid digital credentials and a valid physical ID is given access with the second key.

ID	Weight	Description
6.7	[0.5]	Exam content only accessible with dual authentication (one for student and one for invigilator/system administrator)

5.1.9 Overview of assessment categories and services

The result of the new considerations together with the existing ones, are presented in Appendix C.

5.2 Assessment applied

To make use of the newly adapted security measurement framework, a self assessment form was sent out to key developers of the examination systems in question. The layout of the form is much similar to table in Appendix C, except from the values of the different services. These were left out to avoid any impartial judgement whether these services were a part of the system or not.

Two key developers or project leaders in two different examination systems were contacted and agreed to answer questions and fill out the assessment form. The following table shows an overview of how these two systems, digeks and eExam, answered the self assessment form:

Table 20: Individual scores for reported security services in self assessment

(a) Reported security services for eExam

ID	Security Service	Score
5.1	Access to Internet is restricted/limited by examination system	0.7
5.2	Access with Bluetooth/IR to other devices or networks are completely disabled	0.6
5.4	Access to rogue access points are prohibited	0.6
5.5	Access to internal hard drive is prohibited	0.7
5.6	Access to external hard drives are prohibited	0.6
5.8.2	Secured by implementing procedural security measures to prevent running the system in a virtual machine(e.g. visual inspection at boot time, and/or at periodic intervals during examination)	0.4
6.1.2	Authentication of physical users with ID possible	0.2

(b) Reported security services for digeks

ID	Security Service	Score
1.1	The exam system consists of a distributed architecture	0.3
1.3	Regular backups are ensured by the system	0.7
5.1	Access to Internet is restricted/limited by examination system	0.7
5.2	Access with Bluetooth/IR to other devices or networks are completely disabled	0.6
5.4	Access to rogue access points are prohibited	0.6
5.5	Access to internal hard drive is prohibited	0.7
5.6	Access to external hard drives are prohibited	0.6
6.4	Multiple logins prohibited	0.1

The calculations of the different security levels of the security categories, were done according to the mathematical model of the framework of Eibl et. al in [7]:

$$s_i = \left(1 - \prod_{j=1}^{n(i)} (1 - q_{i,j})^{r_{i,j}}\right)$$

Where $n(i)$ is the number of criteria considered for pillar number i, $q_{i,j}$ is the security criterion value which is in the open interval $[0;1[$ and $r_{i,j}$ is the relevance parameter of each criterion. The relevance parameter is used to describe if the criterion is applicable for the evaluated system and $r_{i,j} \in \{0,1\}$. After these calculations, an overall score were possible to extract. The different scores and the overall score can be seen in the Tables 21(a) and 21(b).

Table 21: Assessment applied for two examination systems

(a) Scores for eExam

Authentication	0.200
Availability	0.000
Non-Repudiation	0.000
Integrity	0.000
Confidentiality	0.000
Authorization	0.997
Overall score	0.199

(b) Scores for digeks

Authentication	0.100
Availability	0.790
Non-Repudiation	0.000
Integrity	0.000
Confidentiality	0.000
Authorization	0.994
Overall score	0.314

Based on the adapted framework, the digeks system achieves somewhat better score than the eExam system. However, both systems did rather poorly in relation to the score range of the framework. By comparing the two systems, we can see that both of them are lacking services to support integrity, confidentiality and non-repudiation. On the other hand, authorization is well covered by both of these systems.

Investigation of implemented security services will be conducted in the following section.

5.3 Testing methodology

Results will be based on investigating security properties identified in assessment of system as well as from the documentation of the system. The main part of the scrutiny will be directed towards the identified services.

In order to measure the level of security offered by a security service, some metric must apply. Some of the security services are difficult to design detailed tests for, and verification through documentation and hands-on tests could be the only way to see if the service is implemented. Because of this lack of scrutiny regarding some of the security services, these can only achieve a maximum of 2 points on our scale, whereas other security services that can be tested thoroughly will get a maximum of 3 points. This maximum indicates that the service works as expected and cannot be exploited within the scope of these tests. A service that achieves a score of 2 is either of such a nature that it cannot be given the same scrutiny or have shown some minor weaknesses. A score of 1 is used where the service shows several or severe weaknesses that can be exploited. A score of 0 indicates that the security service is missing during the tests. We want to clarify the outcome of these tests by presenting the average of all implemented security services by each system. To get an indication of the degree of security coverage by the tested systems, their overall coverage score C is determined as described in the following equation:

$$C = \frac{1}{n} \sum_{i=1}^{n} \frac{s_i}{m}$$

Where n is the total number of security services that exists within the given examination system (determined by self-assessment form sent out to key developers within the projects), and m is the maximum score within the tests. In this case, the services s_i will not get a higher score than 3. The different definitions of the scores can be seen in Table 22.

Table 22: Testing score scale

Score:	**Definition:**
0	Security measure is not present
1	Security measure has several or major weaknesses
2	Security measure has few or minor weaknesses OR Security measure cannot be scrutinized during testing
3	Security measure does not show any weaknesses during testing

When reporting the findings of these tests, they will be presented with both comments on the different security tests that are conducted, as well as how many services and the total coverage degree as exemplified in Table 23.

The basis for the testing is that tests will be carried out for the identified services and the results will primarily tell us something about the security coverage degree. But another point here is to see where the different systems lack in security measures. More precisely, if a security measure is not included in the system, but testing shows that such measure are needed to prevent attacks, this information should also be included in a testing report. E.g. if there is no measure to protect against the use of rogue wireless access points, testing should be conducted anyway to determine if this could be a problem.

Because of this extended testing, an additional metric is needed to tell us how many security services that are not included but should be as they seem to be exploitable according to tests. These "holes" are simply summed to get an overview of how many services that should be investigated further regarding possible implementations, and in Table 23 these are refered to as ”Lacking measures”.

Table 23: Testing result example

System	# services reported	Coverage degree	Lacking measures
System A	xx	xx%	x
System B	xx	xx%	x

To be able to document the process of testing these system, a testing document were drafted for this purpose. The document consists of short guidelines on how to perform testing and with the possibility to fill in scores and comments on the different measures tested. The full testing document can be viewed in Appendix F.

5.4 Test execution

In the following sections, the testing process will be reviewed. Based on this testing, there will possibly be made some discoveries regarding security measures and testing results will indicate the security measure coverage degree.

5.4.1 eExam

The ICT-based examination system eExam initiated from the University of Tasmania were prepared as described in the documentation of the system in [42]. The ISO-image needed were fetched from their site `http://www.eexaminations.org/` and a 4GB USB flash drive from PNY were used in the production of the system. This USB flash drive were partitioned as instructed, and the partition table can be seen in Figure 20.

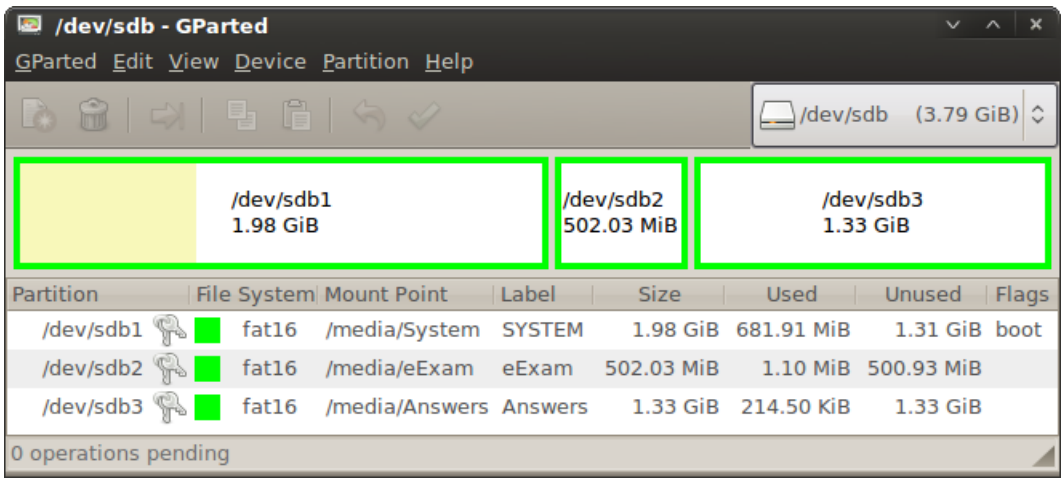


Figure 20: Partitions of flash drive

Also seen in the figure is the bootable system partition which contains the ISO-image, and this startup disk was created with the USB Startup Disk Creator in Ubuntu. As instructed, a background image was placed in the exam partition with the filename ".background.jpg". The system were started by choosing the USB flash drive as the booting device at startup on the test machine. The chosen background image was set as the current wallpaper when Gnome [43] had started.

Network access - Security Service 5.1

The recieved self assessment form indicates that network access is limited as stated in security service 5.1. This statement is also mentioned in the documentation of this examination system.

To test this property, firstly the examination system were booted in a test machine. As network interfaces are rather critical regarding this security measure, these were reviewed first. We listed the hardware and could clearly see that the network interfaces were disabled. Even a hotplugged wireless adapter connected through USB were automatically disabled.

```
ubuntu@ubuntu:/media$ lshw | grep netwo -A 5
WARNING: you should run this program as super-user.
        *-network DISABLED
             description: Ethernet interface
             product: 82566MM Gigabit Network Connection
             vendor: Intel Corporation
             physical id: 19
             bus info: pci@0000:00:19.0
--
           *-network DISABLED
                description: Wireless interface
                product: PRO/Wireless 4965 AG or AGN [Kedron] Network Connection
                vendor: Intel Corporation
                physical id: 0
                bus info: pci@0000:10:00.0
--
  *-network DISABLED
       description: Wireless interface
       physical id: 3
       logical name: wlan1
       serial: 00:13:49:8e:51:86
       capabilities: ethernet physical wireless
```

Figure 21: Network interfaces eExam

Tools such as 'ifconfig' and 'iwconfig' were also unavailable, as it seems that both net-tools and wireless-tools were not installed. The user cannot perform any administrative tasks using 'sudo' either as they are not in the 'sudoers' file. Administrative tools usually available from the system meny were also restricted as seen in Figure 22.

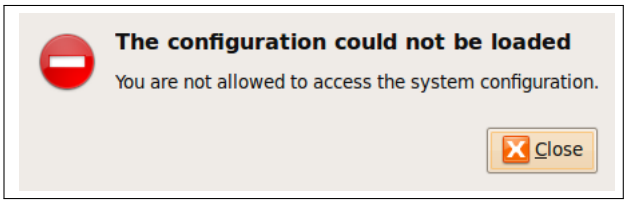


Figure 22: Administration restriction

The only plausible way to bypass this security measure, seems to be by spoofing a legitimate eExam-memory stick.

Example: Spoofing attack

The first problem that arises for an attacker, is that the system uses a custom background image that will change for every exam. This is to prevent the students from using an illegal system during the exam. However, if this image is obtained, it can be applied to any Ubuntu installation.

As a scenario, the attacker might just obtain the image and use it as their own background or copy the picture to a similar but modified memory stick to also simulate a legitimate boot process. The attack is exemplified by the following script in Listing 5.1 which looks for a mounted device in directory "/media/eExam/" and it will copy the file ".background.jpg" to the current location as well as changing the background to the image in question. At least for most invigilators, the system will seem legitimate.

```
1  #!/bin/bash
2  #Script to copy the "hidden" background of eExam to current
3  #+ location and set it as current background
4
5  file="/media/eExam/.background.jpg"
6  let "i = 0"
7
8  while [ $i -eq 0 ]; do
9    if [ -x "$file" ]; then
10     cp -r $file .
11     gconftool -t string -s \
12   /desktop/gnome/background/picture_filename $file
13     let "i += 1"
14   fi
15 done
```

Listing 5.1: Code to obtain image from memory stick

As the boot process might be under surveillance by an invigilator, the attacker might as mentioned copy the image to a less restricted version of eExam. Another possible way to circumvent measure of surveillance for the startup is to record the boot process and present this recording to the invigilator. The script might run in the background and when the video is finished, a valid wallpaper is presented to candidate and invigilator.

Coverage score

The initial testing shows that the wireless and wired network interfaces are disabled in this examination system. They cannot be modified with 'iwconfig' or 'ifconfig' and there is no evident possibility to enable these either. However, there exists trivial methods to circumvent restrictions by spoofing the whole system. For this reason, the coverage score will be 2 in this case.

Bluetooth device communication

The use of bluetooth and IR should be restricted by the examination system. When observing this on the testing machine, 'lsusb' could tell us that the bluetooth device was not disabled as the network interfaces were. However, the proper tools[1] to utilize this device is not installed and thus is lacking the services to support bluetooth communication.

Coverage score

There is no evident possibility that Bluetooth can be utilized through exploitation of the system. The full Bluetooth support depends on the 'bluez'-package and the library to use the Bluetooth protocol stack. This library exists on the system and should be removed to provide an extra layer of security. However, no other weaknesses exists so the coverage score for Bluetooth will be 3.

[1] Usually provided by the package 'bluez-gnome' in Ubuntu

Connection to rogue access points

Coverage score

As explained in security service 5.1, the network interfaces are disabled, so further testing in this service will not provide any useful results. For this reason, no weakness in dealing with rogue access points were found and the score will be 3.

Access to internal hard drive

According to the self assessment form, the internal hard drive should not be accessible for the student. This seems to be true as the device[2] is not mounted at all (verified with 'mount'-command), and it cannot be found in either 'fstab' or 'mtab' files. Additionally, the student user has no possibility to perform super user action with the 'sudo'-command as explained earlier.

Coverage score

Because there is no evident weaknesses that could lead to access of illegal files in the internal hard drive, this security measure gets a 3 in coverage score.

Access to external hard drive

External hard drives should also not be accessible for the student according to self-assessment form, but this seems not to be the case. When confronted with other USB memory devices, the examination system would automatically mount these with read-write permissions as seen in Figure 23.

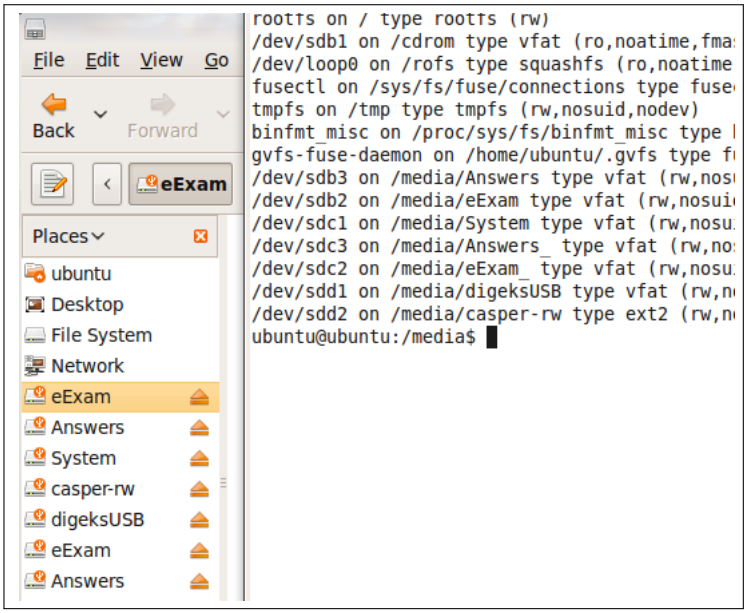


Figure 23: External hard drives mounted

Coverage score

With a total of 8GB of storage in our test case, a lot of illegal information or applications could have been stored to the advantage of a cheating student. For this reason, we consider this weak-

[2]In the case of the test machine, this device was /dev/sda

ness to be severe and have to give a score of 1.[3]

Prevent running system virtually (procedural)

This is a procedural measure to prevent the student from utilizing a virtual machine to run the examination system. Because of the non-technical nature of this measure, not enough scrutiny can be performed in the testing of this so the coverage score will be 2.

Authentication of physical users (procedural)

As with the previous measure, this is also procedural and will get a score of 2 because of this.

Total coverage degree

The testing of the different security services resulted in these coverage degree scores:

Table 24: Coverage scores: eExam

Service #	Name	Score	Vulnerabilities	Tools used
5.1	Network access	2	Spoofing vulnerability	Custom scripts
5.2	Bluetooth access	3	No vulnerability	
5.4	Rogue access points	3	No vulnerability	
5.5	Internal hard drive access	3	No vulnerability	
5.6	External hard drive access	1	File access vulnerability	
5.8.2	Secured by implementing procedural security measures to prevent circumvention by virtualization	2	N/A	
6.1.2	Authentication of physical users with ID possible	2	N/A	

The total coverage degree is then calculated to be 76,19%:

$$C = \frac{1}{7}\left(\frac{2}{3}+\frac{3}{3}+\frac{3}{3}+\frac{3}{3}+\frac{1}{3}+\frac{2}{3}+\frac{2}{3}\right) = 76,19\%$$

Recommendations

The first thing to recommend for improvement is the automatic mounting of new devices through USB. This feature should be disabled, and the only device allowed to be mounted should be the one that boots the legitimate examination system. The application 'polkit-gnome-authorizations' might be of help in turning automount off.

The second recommendation is to further tighten the integrity of the system as little effort is needed to obtain the image that represents the immediate proof of legitimacy for the invigilators. One suggestion would be to look into the access rights of the image and not only depend on security by obscurity in the sense of hiding the picture.

5.4.2 digeks

As with the eExam examination system, the documentation of this system were followed as close as possible to adhere to the default settings of the system and to create a scenario similar to real

[3]It should be noted that the documentation of eExam [42] states the opposite of the claim made in the assessment: "The two key features on this system is to allow access to thumb drives and also set a unique background for the exam. This means that both the exam content and the students answers may be stored on a thumb drive that the students plug into their computers."

life in some Norwegian high schools. As the production environment only runs on Linux and Ubuntu 9.04 was tested and recommended for this purpose, this system was also used in this testing phase.

Installation was done as described in Installation-description of digeks at their wiki [44]. Ubuntu Customization Kit [45] was downloaded and installed together with other required packages. The digeks repository were checked out and the Kubuntu ISO image were downloaded. Following listing shows the procedure for these steps:

```
1 wget http://sourceforge.net/projects/uck/\
      files/uck/2.0.12/uck_2.0.12-0ubuntu1_all.deb/download
2 sudo gdebi uck_2.0.12-0ubuntu1_all.deb
3 sudo aptitude update
4 sudo aptitude install subversion syslinux lilo
5 svn co http://digeks.googlecode.com/svn/trunk/digeks/ digeks-config
6 cd digeks-config
7 wget http://old-releases.ubuntu.com/releases/\
      kubuntu/8.04.1/kubuntu-8.04.1-desktop-i386.iso
```

Listing 5.2: Installation procedure

Next step in the documentation explains how to configure different settings of the system. Most important here was the wireless access setup and the restrictions for accessing web. SSID and keys could be altered to adhere to the local settings, but instead a new virtual wireless access point with the default SSID and corresponding keys were implemented. In this way, reproducibility is better preserved as no configuration files were touched in the process of enabling wireless for the examination system. The same principle were used in case of the configurable restrictions defined by the *kdeglobals*-file. All the necessary restrictions were already in place, so the configuration file were not touched.

To finalize the examination system, instructions to produce the live operating system were followed. First, the customized ISO image is created followed by creating the bootable live USB. The performed commands are listed in Listing 5.3.

```
1 ./uck-cli -d -m
2
3 sudo ./uck-remaster-pack-usb -d /dev/sdb -s casper
```

Listing 5.3: Finalizing the examination system

The system should now be ready for use, and after these last steps were followed, a backup of the USB flash drive were obtained by using the dd utility [46].

Distributed architecture

Both documentation and answer from the assessment form verifies that the examination system is constructed as a distributed architecture, with a student-system and an administration-module. The student-system comprises a USB memory stick which enables booting the modified operating system. The candidates registers after boot with their candidate and room ID to be visible in the administration-module. The administration-module will then provide an overview based on the presence of the candidate on a student-system. The student-system regularly reports back to the administration module about its status.

The behaviour is also observed in the testing phase. When the candidate has registered with their ID, the invigilator has the possibility to approve them in the administration-module. When this is done, the candidate is marked as green which means approved and online. If the candidate reboots or in other ways looses the network connection, they will be marked red and must be re-approved.

One question to ask here is what is preventing a student from using their own modified version of the student-system? The first thing that a student would need to achieve this attack is the key of the wireless access point. If the student got a moment alone with one of the genuine student-systems, all he would do to extract the key is provided in the Listing 5.4 or the full "interface"-file could be copied over to the modified system together with the "serverurl"-file.

```
1 mount /media/digeksUSB/casper/filesystem.squashfs /mnt/squash/ -t
      squashfs -o loop
2 cat /mnt/squash/etc/digeks/interfaces | grep wpa-psk | sed 's/wpa-psk
      //g'
```

Listing 5.4: Fetching wireless network keys

With a strict regime on how these memory sticks are managed before, during and after exams could reduce the vulnerability or the chance to exploit such vulnerabilities, but this method still does rest on some form of security by obscurity.

Coverage score

Due to the observed properties of the student-system which opens for possibilities to spoof a legitimate student-system, coverage score ends up at 2 points.

Regular backups

Regular backups by the student-system could not be verified at the time of testing due to a broken student-system. Several versions of digeks did not handle requests for opening OpenOffice well. For this reason, backup measures could not be tested in detail.

Coverage score

The score will be 2 as detailed tests could not be performed.

Network access - Security Service 5.1

The exam system should have access to the Internet, and after turning on a test machine with digeks on a USB memory stick we could verify that the computer were connected to the Internet by the means of the administration module (test school of NR) at `http://digeksweb.nr.no/adminmod.php`, see Figure 24 for an illustration.

Kandidatoversikt

Kandidat id	Oppetid	IP-adresse	Status	Rom	Siste kontakt	Godkjent klient kl
kand01	**0:07**	77.106.1[redacted]	error	1A	**13:41**	13:48
ads101	**0:52**	77.106.1[redacted]	error	1A	**15:03**	
kand04	0:38	77.106.1[redacted]	ok	1B	14:28	14:22

Godkjenn Fjern

Figure 24: Computer connected and accepted in administration module

However, access to Ordnett and PGSA could not be achieved as we were stopped by an error message proclaiming "You are not authorized to open this file". New installations were produced to circumvent this error, but with no luck as the same behaviour repeated.

With no browser or shell available, some sort of network access seemed difficult to achieve. Probing other applications for holes out of the ”cage” was the last resort in getting some results in this part of the testing. First application to be reviewed was the PDF reader KPDF. Opening some PDF file on a network shared resource would be optimal to prove the success of this attack.

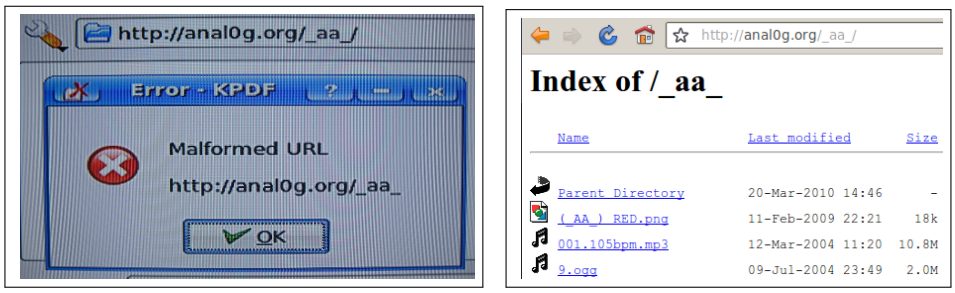
The procedure for opening network resources in our testing was performed as follows:

- Open the given application
- Execute the "File Open"-dialogue[4]
- Try to open folder and files on internal/external web or FTP server

Testing were first conducted against internal web and FTP servers. The result was that access could not be achieved for internal web servers. However, access to a FTP-server running vsftpd [47] on the local network gave no error message. Also, access to subdirectories were possible on this FTP server, but unfortunately listing of files in a directory were not possible and opening files on this server were not possible either.

The next step was to test this behaviour against external web and FTP servers. Same behaviour were confirmed for the web servers, where the application displayed an error message claiming that the URL were malformed. A web page that supported directory listing were chosen, in this case `http://www.anal0g.org/`. KPDF could not view the content of the directory requested, and the error message mentioned were displayed. This error message and some of the actual content of the directory requested can be seen in Figure 25.

Figure 25: Testing access to web server from KPDF



(a) Error message after request

(b) Some of actual content of directory

For the FTP server, an anonymous FTP site in the NO-domain were chosen. More precisely, the first anonymous site in this list were chosen: `http://www.ftp-sites.org/anonymous_ftp_sites_list_no_1.html`. Testing against this server confirmed the local FTP behaviour and it should not be possible as there are measures to prevent this. The security measure implemented

[4]Shortcut CTRL+R might work, or try menu item File -> Open

to mitigate communication over FTP is governed by a configurable rule-set in the file ”kdeglobals” and in a standard installation this rule is set as follows:

"rule_8=open,,,,ftp,,,false"

Which implies that opening an FTP-connection should be rejected. Obviously, these rules does not apply fully to all applications that are installed on the system as KPDF were able to list directories both externally and internally. Figure 26 illustrates this behaviour.

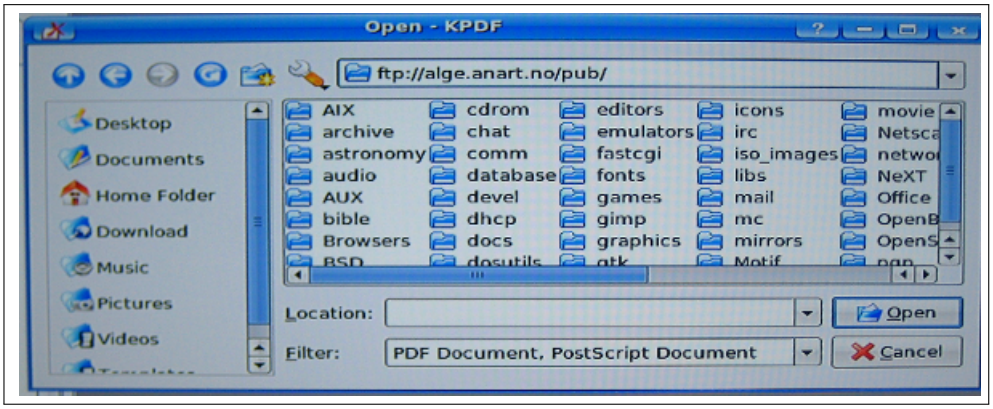


Figure 26: Access to external public FTP server

This can be seen as a covert channel attack, as information can be passed through folder metadata (i.e. names of folders). With the introduction of the EXT file system on Linux, maximum default file name size were extended to 255 characters as mentioned in [48]. The actual files are not accessible, but with a maximum of 255 characters for folder/file names, a lot of information can be stored nonetheless.

The next application that seemed to have some networking capabilities, was the Kaffeine Player which is a media player for KDE. First step was to see if the covert channel behaviour observed with KPDF was similar with this application. There were early confirmation as it was possible to access an external FTP server here as well. The behaviour would probably be similar for all applications that uses the same file manager to open their files, in this case it is Konqueror. In addition to FTP access, the application has capabilities to open media files from the Internet. The web server of `www.anal0g.org` were used this time as well as they are hosting some media files on their server. Two files were tested, first the "001.105bpm.mp3"-file and secondly the "9.ogg"-file as can be seen in Figure 26(b). Kaffeine complained about missing codecs when trying to open the mp3-file, and it asked if we would like the application to look for codecs. After confirming on this matter, nothing happened so installing the codecs seemed to have failed. It did not however complain about illegal accessing of external network resources, which was promising for the attempt of playing some media file. When trying to access the ogg-file, no warning or dialogue boxes were presented. Kaffeine player just started playing the file as seen in Figure 27. It seems that codecs for ogg [49] is better supported than MPEG-based ones [50]. A student might upload the curriculum as an audio file, either presented by the student or if the teacher has done recordings during class, this can be uploaded as well.

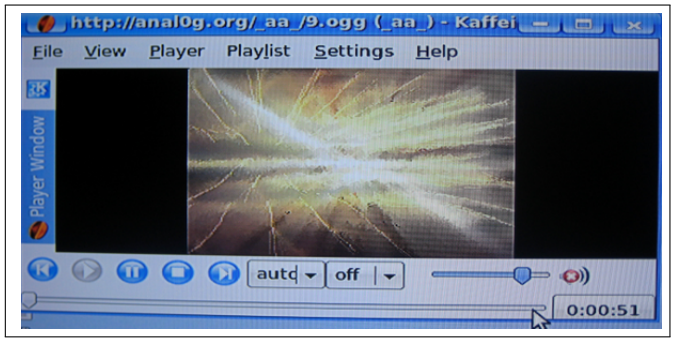


Figure 27: Access to external media file

An assumption to make here is that most examinations does not allow the students to listen to music during the exam mostly to mitigate cheating and/or to reduce noise for other students. The last attack mentioned thus seems to be invalid, but if audio files can be played, how about the video files of ogg? An example video from Wikimedia were tested[5], and Kaffeine would happily play the video for the user as illustrated in Figure 28. This makes the attack extended to the sense that a student can make a video with for example slides from lectures and upload it on a server on the web.

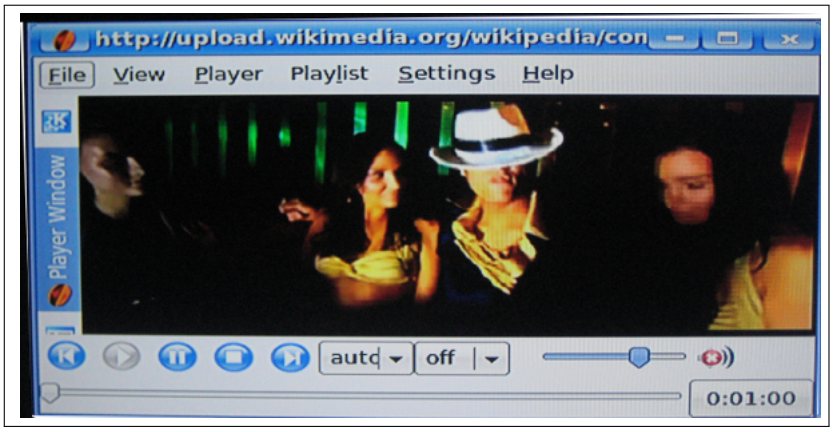


Figure 28: Access to external video playback

Unfortunately, OpenOffice suite rejected to open any of its application, so testing of covert channel behaviour could not be performed on these.

Coverage score

First of all, a covert channel attack with KPDF and FTP is possible. For example, a clever and efficient student wants to help a friend and when he finishes his or hers exam, they can communicate their answers to their less smart or prepared friend by renaming some folders on a public FTP site they are in control of.

Secondly, Kaffeine will play both video and audio files from the web which might enable

[5] `http://upload.wikimedia.org/wikipedia/commons/6/65/Examplevideo.ogv`

students to cheat by uploading curriculum in these file formats on the web before the exam starts.

In addition to the vulnerabilities presented, not all possible attack vectors could be scrutinized (browser were never opened since access to the file were not authorized, and as explained earlier, OpenOffice were also impossible to open in the test environment). In the light of these holes and drawbacks in this security measure, the score will be 1.

Bluetooth access - Security Service 5.2

The first question in this testing to be answered is whether or not the examination computer can be accessed or scanned by the means of Bluetooth technology. If the Bluetooth device is reachable, further testing can be conducted to initiate a session with the device.

Two computers were used in this first stage. The first computer which were running ”digeks” were scanned with the second computer. A tool used to configure Bluetooth connections were used for this purpose, and the full command were ”hcitool scan” which produced no results with the computers approximately 2 metres apart. As a control test, scanning were repeated with another device (a Nokia 5800 cellular phone) which produced similar result regarding the lack of detection of bluetooth device which confirms that the first scan was not a false negative.

The second stage of Bluetooth testing is to investigate if Bluetooth can be activated. In the System Settings of the examination system, early indications were observed that confirmed the suspicion that Bluetooth were completely disabled. When trying to access the Bluetooth-section of the System Settings, an "Empty page" error message were displayed. Additionally, no shell access is available so enabling Bluetooth from shell is also out of the question.

Coverage score

No evident weaknesses were found in testing of this security service and 3 points are appointed accordingly.

External and internal hard drive access - Security Service 5.5 and 5.6

For the external part, the testing were conducted with a USB memory stick and a USB external hard drive. Normally, when plugged into a computer, these devices would present their content in some way to the user. When these devices were plugged into digeks, the examination system will not automatically mount the memory stick or external hard drive and present the files for the student.

From previous testing stages, a covert channel were discovered and used to bypass security measures for communication. In this testing stage, this channel will be investigated towards traversing "illegal" parts of file-system or from mounted media that are not presented visually. As before, the Open-file function of KPDF is used. When trying to access locations outside of $HOME, access is denied and an error message is displayed: "Access denied to file:///etc" (attempted to open folder /etc/). On the other hand, trying to access locations that does not exists, like /foo/, the error message is a bit different: "Access denied to file:///.".

These error messages can be used in the testing of access to external devices by confirmation of a folders existence without permissions to traverse the file hierarchy. The default mount point for Kubuntu/Ubuntu-installations is the /media/-folder, and the aforementioned method confirms that this folder exists. However, when KPDF tries to access the folder that should be

mounted from the USB memory stick, the error message presented indicates that the location does not exist and thus the device is not mounted. The same method were used on an external hard drive[6] with no further luck.

Other methods to traverse the file system or mount the internal hard drive seemed impossible to do as there is no shell access, and no other evident possibility to bypass these restrictions.

Coverage score

There are no evident possibility to bypass any of the security measures set out to protect from mounting external and internal hard drives. For this reason the system get a score of 3 for both these security services.

Multiple logins - Security Service 6.4

Based on the self assessment form, the system does not allow for multiple logins. Testing this security measure requires some assistance from the administration module to see who is getting validated and observing error cases.

The first procedure to test the security measure goes as follows:

- Logging on as ”kand01” on machine 1 and validates this candidate with the administration module.
- Logging on as ”kand01” on machine 2. ”kand01” does not show up twice in the administration module.
- After a minute, the validated ’kand01’ is marked as an ”error”-candidate and is marked as "red".
- After another minute, the ”kand01” can be validated again, but this time it is machine 2 that is validated. This is confirmed by turning off machine 1. The candidate is still "green" after a couple of minutes.

The second procedure is conducted to confirm the first one:

- Same procedure is repeated to confirm the behaviour observed.
- Most of the behaviour were the same, but observations were made about the "kand01" was changing between "red" and "green" status.

The last procedure was control testing to see whether the observed behaviour was due to the fact that the candidate number was the same or if the behaviour was based on the fact that the clients were operating from the same IP address. Earlier procedure were repeated but this time with a different candidate number for the two machines, and this time both of the candidates could be validated. The aforementioned behaviour is thus not a result of the same IP of the clients.

[6] A Western Digital My Book 320GB

Coverage score

First of all, it is not possible for two clients with same candidate number to be validated by the administration module at the same time. However, the observed behaviour opens for DoS-attacks against valid candidates. For this reason, the service get a score of 2.

Rogue Access Points - Security service 5.4

The objective of testing the use of rogue access points is to illustrate possibilities to use an attacker controlled access point for purposes such as man-in-the-middle attacks. The plan was to use tools from the Aircrack-ng tool set [51] to aid in the process of performing attacks on the wireless network to force client to associate with the fake access point. However, as the testing setup used default WPA2 for encryption which is not yet supported by the airbase tool [52], this part of the testing could not be completed as planned.

One other prerequisite for attacks to work could be that the attacker knows the SSID and encryption key used a priori. This could be difficult to achieve if the keys are changed regularly, e.g. after each exam. If such practice does not exist, a procedure to steal the key in an exam setting as explained in Section 5.4.2 could be used.

Coverage score

Because the attack was not possible to perform within the testing environment, no vulnerability to exploit were found and 3 points will be given. However, it should be noted that these attacks could pose as a threat in time or in scenarios where schools chooses wireless networks with weaker encryption.

Total coverage degree - digeks

The testing of the different security services resulted in these coverage degree scores:

Table 25: Coverage scores: digeks

Service #	Name	Score	Vulnerabilities	Tools used
1.1	Distributed architecture	2	Spoofing vulnerability	
1.3	Regular backup ensured by system	2	N/A	
5.1	Network access	1	Covert channel vulnerability	
5.2	Bluetooth access	3	No vulnerability	
5.4	Rogue access points	3	No vulnerability	aircrack-ng
5.5	Internal hard drive access	3	No vulnerability	
5.6	External hard drive access	3	No vulnerability	
6.4	Multiple logins prohibited	2	DoS-vulnerability	

The total coverage degree is then calculated to be 79,17%:

$$C = \frac{1}{8}\left(\frac{2}{3}+\frac{2}{3}+\frac{1}{3}+\frac{3}{3}+\frac{3}{3}+\frac{3}{3}+\frac{3}{3}+\frac{2}{3}\right) = 79,17\%$$

Recommendations

The first element to recommend for improvement is how the administration and student-system communicate in order to establish a verified connection. There are obvious ways to gain access with a spoofed version of a legitimate student-system by stealing necessary credentials like wireless keys, SSID of network and URL of the administration system. A solution which fully prevents

or makes it much harder to spoof the student-system should be looked into.

Discoveries about how different applications could access the network were also made, and a recommendation here is to further tighten the rules which allows or denies network traffic in the student-system. A start would be to look into possibilities to utilize the denying of listing directories which KDE Kiosk supports for several protocols, and some documentation can be found here [53]. Methods of exploiting these holes in the system could be further mitigated by looking into possibilities for security measures that yields defence in depth.

DoS-attack is also possible as long as the attacker has acquired the key of the access point and know the candidate number of the target student. Mitigation to prevent this must be considered.

5.4.3 Additional testing

Additional testing is necessary to include threaths not covered by security measures reported in the assessment. This will help us map the lacking measures mentioned earlier. For the main part, this encompasses the virtual machine threat for both systems. The threat can be defined as the possibility for a student to run the examination system in a virtual machine to bypass one or more security measures. The system owners of both digeks and eExam are aware of this threat as they mention the possibility for such attacks in their documentation. The contact person from eExam also mentioned procedural measures to prevent this in the assessment, while the digeks project team have mentioned this in several of their papers on digeks [9, 19]. In order to test the severity of this threat, two virtual machine software were used for this purpose; VMWare Workstation [54] and QEMU [55].

Virtual machine testing - eExam

The eExam system were tested first in VMWare Workstation. The image used to produce the system is also used as an image to boot in the virtual machine. The first problem to encounter is the missing background image. Since the system does not find the background image in the exptected partition, the system freezes and prompts an error message. See Figure 29 for an illustration.

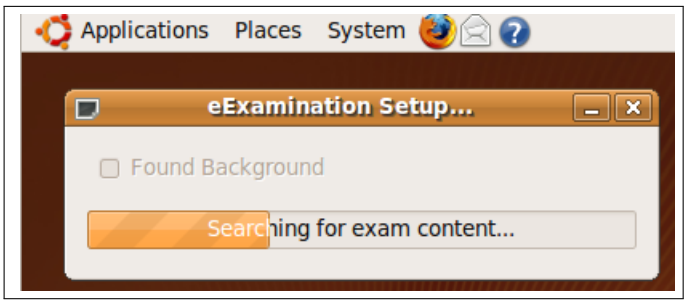


Figure 29: Expected background image missing

To encompass this problem, we used the already configured USB memory stick containing eExam. When connecting this device to the virtual machine, the correct partition were found and the background image were set. As some noisy ad-hoc configurations were needed to accomplish the attack[7], an easier approach were found by instructing the virtual machine to automatically

[7]Instruct Vmware to mount the device and confirm this action.

connect the USB devices at boot. The USB device had to be unmounted at the host operating system in order to be automatically mounted in the guest operating system. To further increase the stealth-level of the attack, the disabling of automounting in the host operating system were conducted as explained in Section 5.4.1.

The testing have shown that running the examination system eExam in a virtual machine is possible and unskilled personnel can have problems to determine if the system running is virtual or not. Further testing with other virtualizers is not needed as the attack were successful.

Virtual machine testing - digeks

In order to extract a copy of the digeks examination system, an image was created with the dd utility. This image was first booted in VMWare Workstation as a floppy disk image only to produce a disk read error. Other attempts with booting the image after it has been mounted in the host operating system did not work either.

Next step was to try to boot the image in qemu. The test machine were running Ubuntu 9.04 with QEMU version 0.10.0. The boot process looks normal, but it ended abruptly with an I/O-read error. Another laptop with Ubuntu 10.04 and QEMU 0.12.3 were tested, but the process cancelled even earlier with a permission denied error regarding startup-scripts for the digeks system.

From testing with two different virtual machine applications, no virtual machine attack could be completed against digeks. However, as the virtual machine seem to fail at different stages in the boot process with different versions of the virtual machine software some promise for this attack to succeed with other configurations is seen. Additionally, the people behind digeks have obviously run the system in virtual machines as seen in one of their publications [9].

5.5 Testing results

The full testing phase provided us with the results presented in Table 26.

Table 26: Testing result table

System	# services reported	Coverage degree	Lacking measures
eExam	7	76,19%	1
digeks	8	79,17%	(0)[11]

[11] Virtual machine threat could not be exploited, but showed promise to do so with future versions of virtual machine software or different configurations.

6 Proposed framework

In the following chapter, the proposed framework for ensuring security when conducting ICT-based examination is presented. The framework is a result of experiences from testing two examination systems as well as feedback from system administrators in Norwegian high schools in a survey regarding ICT-based examinations and security.

The different elements of the framework should give a good starting point on how security is best preserved in these settings, and more detailed implementation guidelines will be presented in the next chapter.

6.1 Authentication

The process of authenticating people or entities is often seen as the first visible security measure of a system, and it often enables the possibility for other security measures to function such as access control and integrity/confidentiality measures.

6.1.1 Password based authentication

In the testing phase, it was observed that none of the examination systems had implemented any form of username and password combination scheme. Instead, eExam replied in the assessment that they used a more traditional form of identifying students based on physical ID. An identification is done in digeks as well, but instead of physical ID, the student users are requested to fill out their candidate number and the classrom for their examination.

The procedures that are used for authentication, leaves a lot of responsibility on the invigilators to determine the correct identity of the candidates. One might assume that this practice is a result of trying to mitigate that candidates exchanges usernames and passwords as was reported as one of the observed cheating incidents in the survey.

Requirement 6.1.1:

> A combination of authentication with physical identification and logical identification is preferred as cheating incidents where exchanging exam identities have better promise of being prevented.

6.1.2 Multiple logins

As seen in the testing stage, it was not possible to have two clients validated at the same time with the same candidate number in the digeks system. However, a mischievous student might make a lot of problem for another student by posing with the same candidate number. This attack will invalidate the first student, and on next validation the attacker is validated. Different scenarios of the attack can be carried out, either as a directed DoS-attack as described firstly here, or as a spoofing attack where an accomplice of a cheating student validates their client on behalf of the student. The invigilator might be of the impression that the candidate is behaving properly since it is marked as valid with the colour green.

To avoid the first scenario, another attempt to join with the same candidate number as an already validated client should be blocked. The second scenario might be harder to avoid as the accomplice could be the first to be validated, but since the accomplice is presumably not present in the examination room, a solution where some form of two-party-authentication (student and invigilator) is preferable in order for the candidate to join the network/examination. I.e. the authentication is only possible with the presence of the invigilator in collaboration with the candidate.

Requirement 6.1.2:

Multiple logins should explicitly be blocked. Use invigilator-enabled authentication to prevent spoofing attacks.

6.2 Access control

Controlling access to different resources are closely connected to the mitigation of cheating. For this reason, accurate access control is paramount to obtain a satisfying level of security.

6.2.1 External/internal drive access

About a third of the schools were concerned about external and internal resources on the student computers, whereas 14,6% were reporting that they actively blocked the use of memory sticks/external hard drives to mitigate cheating. Disabling mounting of devices, both external and internal, effectively blocks this possibility to cheat. This was seen in the testing of digeks where no devices could be mounted, whereas in eExam where this was possible and the examination candidate had access to files on devices he or she had brought to the exam. Some minor patches of this mounting functionality should fix this issue.

Requirement 6.2.1:

Mounting devices should be disabled, both for external and internal drives.

6.2.2 Network access

As seen in the survey, blocking illegal communications is seemed as one of the most significant security challenges in the ICT-based examination setting. Not surprisingly, in a setting where no Internet is needed seems to be easier to handle as opposed to a system where there is a requirement for limited access to network resources. When these limitations cannot be ratified in a satisfying manner, illegal communication will occur and cheating incidents will happen. Most (about 60%) of the cheating incidents reported in the survey were related to misuse of network access.

Access to Internet should be enabled only when strictly necessary and only for specifically allowed resources needed to complete the examination. The previous statement was followed in the design of the digeks examination system, but due to certain assumptions in the implementation, not all applications were covered by the rule-set that should enforce the access control in a whitelist fashion. The default PDF-reader and the Kaffeine media player had access to network resources that should have been blocked. An addition to the first statement should be that all applications should be included by the network resource limitations set out by the system.

Where the exam situation allows for it, blocking all access to Internet should be the prefered solution. The examination system eExam blocks this communication by disabling all network

interfaces, and thus students cannot cheat by connecting to nearby wireless access points or by other ways mitigating network access security measures.

Several layers of security is important in many areas of security, and it is no exception here. From the survey, it is seen that about 86% of the schools are using a form of surveillance of the students in some, medium or high degree. These schools have better chance of detecting the covert channel attack found in digeks. Mitigating the attack could also be done by using a properly configured firewall. Half of the schools reports that they use the firewall to prevent the illegal communication among examination candidates, but there is no guarantee that these firewalls have all the rules in place to do this.

The main point to extract from this is that every possible application that is a part of the examination system must also be a part of the limited or no access scheme.

Requirement 6.2.2:

> If network access is necessary, restrictions that apply must encompass all applications that can be used at the client. Also, restrictions should also be implemented at the network layer to provide defense in depth.

6.2.3 Bluetooth access

About 4 out of 10 schools reports that they are blocking this kind of communication to mitigate cheating. This also means that about 60% of the schools have not explicitly blocked Bluetooth usage, which could enable the students to use illegal resources or communicate illegally. None of the systems in the testing phase had any possibility to use Bluetooth, and as both communication and use of external resources is possible with this technology, a requirement to prevent the use of it is needed.

Requirement 6.2.3:

> The Bluetooth device should be disabled on the system, and it should not be possible to reactivate it for use during the examination by the student.

6.2.4 Application access

Over half of the schools that have used ICT-based examinations allows all kinds of applications to run on the computers during the exam. While not a part of this thesis assessment and testing phase, the lack of restrictions on which applications that could be used while conducting the exam is of somewhat concern especially in foreign languages were misuse have been reported. The tested examination systems have, as default, a certain set of programs included to aid the students in completing their examination answer. As long as the student does not gain privileges to install new applications, this limitation to a certain set of programs is preferable.

Requirement 6.2.4:

> Access to applications should be limited to those necessary to complete the examination.

6.2.5 Rogue Access Points

About two thirds of the schools reported use of wireless access for the students during examination. From the testing we have seen the importance of how wireless keys are managed and the strength of the encryption matters as well. It proved difficult to attack the wireless with WPA2-encryption. However, attackcs would have better promise if the different schools choose to use

protocols that yields weaker level of encryption.

Requirement 6.2.5:

When wireless networks are used, WPA2 is the prefered protocol.

6.2.6 Accessing system virtually

As seen in the testing phase, students could possibly use the examination systems in a virtual machine. With eExam this was fully possible, but running digeks proved to be harder. The virtual machine threat must be considered severe as the attack could enable the candidate to circumvent all or many of the current security measures.

Requirement 6.2.6:

Implement technical measures to prevent running the examination systems as a virtual machine.

6.3 Confidentiality

None of the tested systems have reported specific measures to preserve the confidentiality of data during an exam. Over half of the schools in the survey reported that they did not use any form of encryption of exam questions and answers. Furthermore, several respondents proclaimed that it was the external system who provided the questions that were responsible for this encryption. Requirement regarding confidentiality cannot be defined when no testing regarding this security category have been done and at the same time it is questionable if the examination system have any advantages in increased security by encrypting either student documents or questions.

6.4 Integrity

There are two aspects of integrity in this case. First of all the integrity of the exam answer of the student, and second is the integrity of the examination system. The integrity of the examination system has received more focus than the examination documents in this thesis as the main goal is to investigate security of the systems mainly. Integrity is well covered within the requirements in security category of Authorization/Access control. These requirements will help enable the desired level of integrity of the system.

6.5 Availability

One of the tested systems consisted of a distributed architecture and this is the only point that has touched the subject of availability. However, the distributed architecture of digeks has not the object to provide higher availability but more of attestation of system integrity of the different systems connected to the administration module. Planned testing of backup routines of digeks could not be fulfilled at the time of testing, but it is clear that the information that the student provides in form of examination answers should be secured from accidental or intentional deletion or modification of this.

6.6 Non-repudiation

Non-repudiation is poorly confronted by both the respondents of the survey as well as the assessment phase in this master project. The reason for this lack of focus in non-repudiation seems

to be the fact that this property is mostly ensured by external parties. Thus we does not find it useful at this point to define requirements if this as it is covered by other parties in this context.

7 Implementation possibilities

This chapter will look into what kind of mitigation techniques, software, protocols and tools are needed to adhere to the requirements of the proposed framework presented in Chapter 6. As the proposed framework is based on both testing and the best practice survey, elements from those phases will be the focus of this chapter.

7.1 Authentication

Two main requirements for authentication is derived based on testing and survey. These requirements can be seen below:

- A combination of authentication with physical identification and logical identification is preferred as cheating incidents where exchanging exam identities have better promise of being prevented.

- Multiple logins should explicitly be blocked. Use dual authentication to prevent spoofing attacks.

There exists some alternatives that either supports one or both of these requirements. One of these alternatives is to look into the possibility to implement a Kerberos-like [56, 57] protocol to authenticate users for communication between administration module and the clients. The clients on the memory sticks can for example be configured to use OpenLDAP [58] to look up the examination users.

One of the problems in the authentication phase is the possibility for spoofing. Spoofing is not directly mitigated with the use of Kerberos as the student still can give his or her credential to an accomplice. To mitigate these spoofing attacks a form of physical and logical authentication combination with a threshold password scheme could be used. Shamirs secret sharing [59] scheme is an alternative that would fulfil this purpose. This scheme was developed to cope with situations where a certain threshold of key holders is needed to unlock a secret, in this case it will be a 2-out-of-2 or 2-out-of-3-threshold where both student and invigilator or examination administrator most produce their credentials.

Another approach is to use port based authentication with 802.1X and digital certificates where the certificates are locked/encrypted until both the candidate and an invigilator has provided their password. The secret sharing scheme of Shamir mentioned above could be used here as well, and to prevent brute force attacks in this scenario time delay between authentication attempts could be implemented. The student acts as the *supplicant* (See Figure 30) and wishes to connect to the Internet via the Wireless Access Point which acts as an *authenticator*. The job of the authenticator is to act as a security guard or gate to the protected network [60].

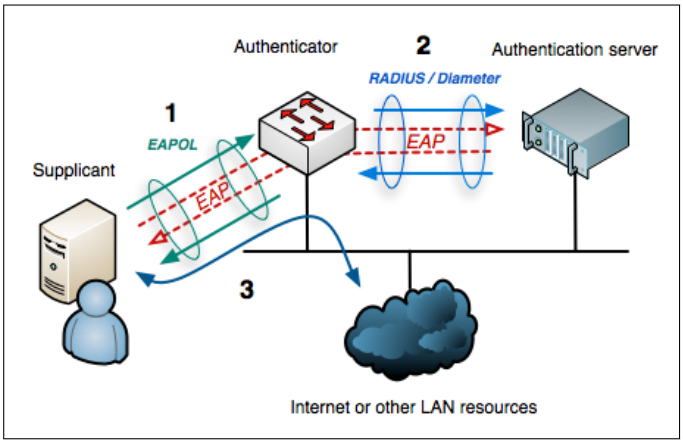


Figure 30: 802.1X port based authentication[1]

The authenticator makes sure the gate is closed until the *authentication server* verifies the supplicant credentials. What type of authentication server used is up to the different schools, but the RADIUS server is most commonly used [60].

7.2 Access Control

There are three requirements regarding access control derived from the testing phase. The first requirement covers local devices connected to the computer. The second requirement covers external resources and communication provided by network access, and the last requirement covers the virtual machine threat.

- Mounting devices should be disabled, both for external and internal drives.
- If network access is necessary, restrictions that apply must encompass all applications that can be used at the client.

Both of the test systems claimed that they were blocking access to external USB memory devices. One of these systems had not implemented this measure properly as it was possible to read any information from these external devices when connected. The PolicyKit [61] of Ubuntu could be used to define this rule. The concerning rule is usually found in `/usr/share/PolicyKit/policy` or in `/usr/share/polkit-1/actions` for newer Ubuntu systems.

There is a need for providing layered security for the control of the network access. Uncontrolled access to Internet or the Intranet can provide for communication between students or the use of other illegal aids. A holistic approach as proposed in [62] where protection is applied on the network layer, on the host itself and at the application layer could be adapted for this purpose. Based on the testing phase, the protection at the application layer to prevent unauthorized access to network resources were too weak. A more strict default rule-set which also handles the denial of listing of directories would be recommended to further tighten the network access. Additionally restrictions based on measures at the host could include a host-based firewall such as ufw [63]. The rule set of this host-based firewall could be a part of the configuration done before producing the live operating system.

The last requirement covers the virtual machine threat described in Section 5.4.3 and is stated as follows:

- Implement technical measures to prevent running the examination systems as a virtual machine.

The requirement is only useful if it can be implemented in the examination systems. The question is, how does the system detect that it is running in a virtual machine? Jon Galloway explains in his article [64] two possible methods to perform this detection.

The first technique is called direct hardware fingerprinting and it exploits the fact that virtual machines obtain specific hardware related to the VM software. For example, hardware identified as manufactured by Virtualbox or VMware is highly likely contained inside a virtual machine running VM software from one of those product vendors. Ben Armstrong has written a short article [65] about using this technique to detect if the machine is running inside a virtual environment by Microsoft. The script he presents, probes for motherboard vendor which in this case will be Microsoft if the system is virtual.

The second technique is called inferred hardware fingerprinting and it exploits the changed behaviour of some hardware elements. Certain system calls can be made to determine if there is a virtual machine present. Some researchers at SecuriTeam have written an article [66] about how this can be done for VMware by making a system call to a VMware specific I/O port. Some proof-of-concept code have been developed by the same people with this functionality and with some slight modifications this small detection program could detect eExam running inside a VMware virtual machine. The slightly modified proof-of-concept code can be seen in Appendix D and the test run in eExam can be seen in Figure 31.

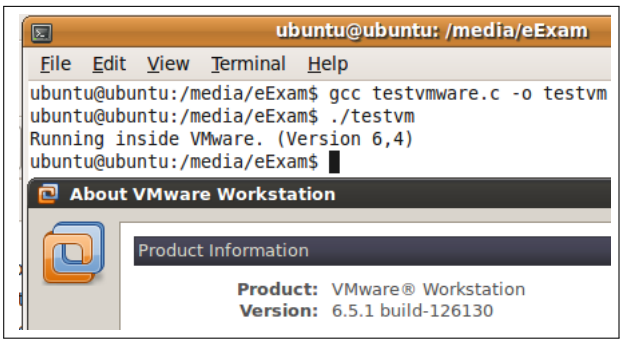


Figure 31: Detection of VMWare host in eExam guest

The detection and detection prevention have been a cat and mouse game in the last decade, most notably with the introduction of BluePill [67] and some of its critics [68, 69, 70]. The exercise of testing if direct or inferred hardware detection can be circumvented is however outside the scope of this thesis.

8 Conclusion

This chapter will review through discussion what has been achieved in this master project. A conclusion will be made to sum up the project and the chapter will also include a section which discusses future possibilities in this research area.

8.1 Discussion

Discussion of both survey results, assessment and testing results will be conducted.

8.1.1 Survey

Ensuring the correctness of conducting ICT-based examination is perhaps the main motivation for researching security in this context. The survey was conducted to get an image of how security are preserved in these settings. A low number of cheating incidents per year would give an indication of a certain correctness, and the result of the survey does indeed indicate a low number of cheating incidents based on reported incidents from the schools. There are only 2 incidents per 1000 students reported yearly.

The reported number of incidents and the actual number of incidents might however not be the same. In fact, in the aforementioned Universitas-survey they concluded that 9 out of 10 cheaters in a Norwegian University are not caught and thereby not reported. Many of the properties of the population they investigated correlates with high school student properties[1], and this could possibly mean that 20 out of 1000 students in high school cheats on the exam. A dark figure study on the matter could have shed some light regarding the real cheating incident rate in these schools. This was however not prioritised within the time frame of the master thesis.

When looking for association between students using their own computer and reported incidents, we observed that there are significantly less reported incidents in these cases. This observation was based on either filtering where only schools connected to Internet was included or regrouping the incidents group into observed/not-observed. The first thing in mind when observing this, is to explain it by the lack of control when students use their own computer. I.e. as an effect of lacking control, fewer incidents are reported. A different explanation would be that fewer incidents are reported because the students in these cases tend to cheat less, maybe because of the increased freedom they take more responsibility. But the latter explanation here does not explain the possible dark figures mentioned earlier and the former does.

More control equals more reported incidents as we have seen, and this should imply that if an increase of surveillance level occurs, incidents reported will also increase. There is however no statistical significance that support the hypothesis that more surveillance coincides with more reported cheating incidents. The incident rate even drops from some to medium degree of surveillance as seen in Figure 18.

[1] Cultural properties, geographical properties and age (with some years apart)

The invigilators are the most used mitigation method to prevent cheating and they are also the biggest security challenge due to their lack of technical knowledge. Invigilators are seemed as not capable of performing good supervision of students when ICT-based examinations are used. The immediate observation here is that these often unskilled persons are given too much responsibility regarding the students in the ICT-based examination scenario.

Both terms like non-repudiation and availability are misunderstood or not comprehended by some of the respondents in the survey. One reason for this might be that the statement of the question is unclear and further explanations should be given. In the case of non-repudiation this should be clear as the term was explained with an example within this certain context.

8.1.2 Assessment and testing discussion

We have based the assessment on an existing assessment framework for e-learning systems. The added security services/measures in the adopted assessment framework have been subject for an evaluation to appoint the different score values. This evaluation is subjective in nature and the score might change if someone else would appoint these values. For this reason, the overall score given to a system cannot conclude with absolute certainty that this score depicts the actual level of security in the ICT-based examination system. However, the overall score will provide good pointers for where the examination system is well equipped and where the system need some more attention.

The results from the assessment provided information such as focus areas for implementing security measures. The prevalent focus area for security was without doubt access control where both systems gained a high score as a result of several security services here. As an effect of lacking in services in the other categories, both systems achieved a rather low overall score after the assessment. The eExam ended up with 0.199 and digeks ended up with 0.314, which in both cases is not very impressive. However, these examination systems might differ from the systems that the original assessment framework were developed to assess. For this reason, a weighting of the different security categories can be used as a part in future development of this assessment framework.

Testing of every single security service would be both unnecessary and cumbersome, because testing the strength of a security measure that does not even exists is a waste of time and resources. We chose to mainly focus on the mapped services from the assessment phase. By doing this, we knew that the service was supposed to be there and testing of it would not be a waste of time. In addition to the mapped services, we also chose to consider the virtual threat in the testing phase as both systems have in some way mentioned this as a problem.

The services are given a score based on how well they perform during the testing exercise. A system which shows no specific vulnerability get a full score and a service showing several or severe vulnerabilities achieves a low score. The testing methodology gives a clear mental image of the total score for a system based on the total coverage score calculated and presented in percentages.

There are some reasons to criticise this method as well since the test execution, and hence the results, might be influenced by the skill level of the executor. The test document gives some guidelines on how to carry out the experiments, but there are of course possibilities of misinter-

pretation or giving too much attention on one item and too little on the next. These risk elements would in some degree be a part of any testing methodology and thus is difficult to circumvent this human factor.

Based on the testing results, very little separates the two examination systems. Both of the systems show one severe vulnerability in one of their security services, and minor vulnerabilities in some of the other services. Digeks achieves a score of 79,17% and eExam is close behind with 76,19%. These scores reflects the fact that they are both solid systems for conducting ICT-based examinations but both of them have also some areas of possible improvements.

8.2 Future work

Improving the method for assessment and testing of ICT-based examination systems should be considered in future work on this matter. We have seen that the assessed and tested systems achieved poor results in the assessment. There is no different weights for the different security categories in the assessment and the potential for improvement might be to concentrate more of the effort regarding access control as this is the main goal, namely to control the access of the students to prevent illegal activities during the examination.

Another future work for this area is to develop an ICT-based examination systems that implements security functionality based on requirements proposed in our security framework. Assessment and testing should also be conducted for these systems to compare with already assessed and tested versions of digeks and eExam. Comparisons could also be extended to include commercial products that promise similar functionality and security levels.

Other approaches should investigate methods to increase the interoperability between the security services offered by the examination system and external systems, as the aforementioned PGS which provides security services as well. A more closely connected authentication scheme between these could decrease the attack surface.

The survey we have conducted is not accurate enough to determine how many of the students cheating on the exam per year, and to achieve this more accurately, a dark figure study can be a solution. This survey should include students from several high schools to get an overview of how widespread this problem is and what methods are used to circumvent the security measures implemented. This survey could be executed before and after the implementation of a system based on some of the requirements proposed in this thesis in order to see the effect of these measures.

8.3 Conclusion

In order to investigate the best practice of ICT-based examinations and their security properties in educational institutions, observations have been made from a survey sent out to IT-administrators in Norwegian high schools. A good overview of how security is conceived and handled at these schools have been the result of this survey.

By assessing and testing the two examination systems, we have found certain security areas which needs attention and we have developed some requirements in these areas which should be prioritized when developing new examination systems or increasing the security in already deployed systems. The methods of assessment and testing can also contribute by acting as a

guideline for how these activities can be performed.

In the aftermath of proposing new requirements for examination systems, we have contributed by looking into possible solutions in order to comply with these requirements. Implementing a Kerberos-like protocol for authenticating users in combination with a secret sharing scheme to prevent spoofing attacks is one of these suggestions we have made. The implementations itself was not fully investigated by developing prototypes with these protocols and measures, but as suggested in Section 8.2 this should be considered in future endeavours with ICT-based examination systems.

Bibliography

[1] Cudbard-Bell, A. 2010. Diagram showing protocols involved in wired 802.1x authentication. `http://en.wikipedia.org/wiki/File:802.1X_wired_protocols.png`. Last visited 2010-05-31.

[2] Marais, E., Argles, D., & von Solms, B. 9 2006. Security issues specific to e-assessments. In *8th Annual Conference on WWW Applications, Bloemfontein*.

[3] Apampa, K. M., Wills, G. B., Argles, D., & Marais, E. 2008. Electronic integrity issues in e-assessment security. In *ICALT*, 394–395.

[4] Mrabet, R. & Kettani, M. E. 1998. Edile : Exam distance learning environment. *Continuing Engineering Education, 7th World Conference on*, 195–199.

[5] Weippl, E. R. 2005. *Security in E-Learning*, volume 16 of *Advances in Information Security*. Springer.

[6] Weippl, E. 2005. Security in e-learning. *ACM eLearn*, 2005, 3.

[7] Eibl, C. J., von Solms, B., & Schubert, S. 2006. A framework for evaluating the information security of e-learning systems. In *Information Technologies at School. Proc. of ISSEP 2006, Inst. of Math. and Inf., Vilnius, Lithuania*, 83–94.

[8] Herrera-Joancomartí, J., Prieto-Blázquez, J., & Castellà-Roca, J. 2004. A secure electronic examination protocol using wireless networks. *Information Technology: Coding and Computing, International Conference on*, 2, 263.

[9] Fretland, T. & Leister, W. 12 2008. Sluttrapport: Utvikling av teknologi for digital eksamen. *Norsk Regnesentral: DART/02/08*.

[10] Fluck, A., Pullen, D., & Harper, C. 9 2009. Case study of a computer based examination system. *Australasian Journal of Educational Technology*, 25(4), 509–523.

[11] Castella-Roca, J., Herrera-Joancomarti, J., & Dorca-Josa, A. 2006. A secure e-exam management system. *Availability, Reliability and Security, International Conference on*, 0, 864–871.

[12] Kambourakis, G., Kontoni, D.-P. N., Rouskas, A., & Gritzalis, S. 2007. A PKI approach for deploying modern secure distributed e-learning and m-learning environments. *Computers and Education*, 48(1), 1 – 16.

[13] Furnell, S., Onions, P., & Bleimann, U. 1998. A security framework for online distance learning and training. *Internet Research*, 8(3), 236 – 242.

[14] Kritzinger, E. 2006. Information security in an e-learning environment. In *Education for the 21st Century*, 345–349.

[15] Ko, C. & Cheng, C. 2008. Flexible and secure computer-based assessment using a single zip disk. *Computers and Education*, 50(3), 915 – 926.

[16] Canonical. 2010. Ubuntu. `http://www.ubuntu.com/`. Last visited 2010-05-20.

[17] Fluck, A. & Hesketh, J. 2010. eexam project page. `http://www.eexaminations.org/`. Last visited 2010-05-24.

[18] Hesketh, J. 2009. eexams on computers - update. `http://www.opentechnologysolutions.com.au/news/eexams-computers-update`. Last visited 2010-05-24.

[19] Leister, W., Fretland, T., & Solheim, I. 11 2009. Preventing unwanted communication in ict-based exams by using free software. In *NOKOBIT 2009*.

[20] Canonical. 2010. Kubuntu. `http://www.kubuntu.org/`. Last visited 2010-05-20.

[21] Webber, C. G., de Fátima Webber do Prado Lima, M., Casa, M. E., & Ribeiro, A. M. 2007. Towards Secure e-Learning Applications: a Multiagent Platform. *JSW*, 2(1), 60–69.

[22] Webber, C. G., De Fatima, M., Do Prado Lima, W., Casa, M. E., & Ribeiro, A. M. 2006. Adding Security to a Multiagent Learning Platform. In *ARES '06: Proceedings of the First International Conference on Availability, Reliability and Security*, 887–894, Washington, DC, USA. IEEE Computer Society.

[23] Ward, A., Roca, J. C., & Josa, A. D. 2007. Designing a cryptographic scheme for e-surveys in higher-education institutions. *Availability, Reliability and Security, International Conference on*, 0, 1251–1255.

[24] Chadwick, D. W., Tassabehji, R., & Young, A. 2000. Experiences of using a public key infrastructure for the preparation of examination papers. *Comput. Educ.*, 35(1), 1–20.

[25] Weippl, E. & Tjoa, A. M. 2005. Privacy in e-learning: Anonymity, pseudonyms and authenticated usage. *Interactive Technology and Smart Education (ITSE)*, 2005(2), 247–256.

[26] Skolehjelperen. Norwegian high school list. `http://www.skole.no/skoler/skoler.php?type=vgs`. Last visited 2010-05-30.

[27] Østtveit Barbogen for Universitas, H. 3 2010. 1 av 20 har jukset på eksamen. `http://universitas.no/nyhet/54732/1-av-20-har-jukset-pa-eksamen/`. Last visited 2010-05-23.

[28] Utdanningsdirektoratet. 2010. Skolefakta - elevar, lærarar, skolar. `http://skoleporten.utdanningsdirektoratet.no/rapportvisning.aspx?enhetsid=00&vurderingsomrade=fed86d60-df13-45c8-a544-457b84fc8216&skoletype=1`. Last visited 2010-05-14.

[29] Utdanningsdirektoratet. 2010. Informasjon om eksamen våren 2010. http://utdanningsdirektoratet.no/Artikler/_Eksamen/Informasjon-om-eksamen-varen-2010. Last visited 2010-05-14.

[30] Utdanningsdirektoratet. 2010. Ikt-basert eksamen våren 2009 (midlertidig brukerveiledning 10. mai 2010). http://www.udir.no/upload/Eksamen/Eksamensansvarlig_Brukervl_IKT_basert%20eksamen_Midlertidig.pdf. Last visited 2010-05-14.

[31] Utdanningsdirektoratet. 2010. Bruk av datamaskin til eksamen i kunnskapsløftet. http://www.utdanningsdirektoratet.no/Artikler/_Eksamen/Bruk-av-datamaskin-til-eksamen-i-Kunnskapsloftet//. Last visited 2010-05-14.

[32] Utdanningsdirektoratet. 2010. Hjelpemidler til eksamen i kunnskapsløftet. http://www.udir.no/Artikler/_Eksamen/Hjelpemidler-til-eksamen-i-Kunnskapsloftet/. Last visited 2010-05-14.

[33] Anderson, R. J. 2008. *Security Engineering: A Guide to Building Dependable Distributed Systems*. Wiley, 2 edition.

[34] Saltzer, J. H. & Schroeder, M. D. 1975. The protection of information in computer systems. *Proceedings of the IEEE*, 63(9), 1278–1308.

[35] Lampson, B. W. 1973. A note on the confinement problem. *Communications of the ACM*, 16(10), 613–615.

[36] Bryans, J. & Arief, B. 2007. Security implications for structure. *Structure for Dependability: Computer-Based Systems from an Interdisciplinary Perspective*, 217 – 227.

[37] Landwehr, C. E. 2001. Computer security. *Int. J. Inf. Sec.*, 1(1), 3–13.

[38] Murdoch, J. 2006. Security Measurements - Prepared on behalf of the PSM Safety and Security TWG.

[39] Savola, R. 2006. Towards security evaluation based on evidence collection. In *Proceedings of the 3rd International Conference on Fuzzy Systems and Knowledge Discovery (FSKD)*, volume 4223 of *Lecture Notes in Computer Science*, 1178–1181. Springer.

[40] Jones, A. & Ashenden, D. 2005. *Risk Management for Computer Security: Protecting Your Network & Information Assets*. Butterworth-Heinemann, Newton, MA, USA.

[41] Fretland, T. & Leister, W. 2010. Digeks project page. http://code.google.com/p/digeks/. Last visited 2010-05-24.

[42] Hesketh, J. & Fluck, A. 2009. eexamination trial system - revision 2. http://www.educ.utas.edu.au/users/afluck/eExaminations/download/eExam2-docs.pdf. Last visitied 2010-05-22.

[43] Gnome. 2010. Gnome homepage. http://www.gnome.org. Last visited 2010-05-20.

[44] Fretland, T. Digeks - wiki. http://code.google.com/p/digeks/wiki/Overview. Last visited 2010-05-30.

[45] Balliano, F., Farkas, S., & Lichota, K. Ubuntu customization kit. http://uck.sourceforge.net/. Last visited 2010-05-30.

[46] Gnu. dd: Convert and copy a file. http://www.gnu.org/software/coreutils/manual/html_node/dd-invocation.html. Last visited 2010-05-29.

[47] Evans, C. vsftpd official home page. http://vsftpd.beasts.org/. Last visited 2010-05-30.

[48] Card, R., Ts'o, T., & Tweedie, S. Design and implementation of the second extended filesystem. In *Proceedings of the First Dutch International Symposium on Linux*, number ISBN 90 367 0385 9. Laboratoire MASI — Institut Blaise Pascal and Massachussets Institute of Technology and University of Edinburgh.

[49] xiph.org. Ogg vorbis official home page. http://www.vorbis.com/. Last visited 2010-05-30.

[50] MPEG. Mpeg official home page. http://mpeg.chiariglione.org/. Last visited 2010-05-30.

[51] Aircrack-ng. Aircrack official home page. http://www.aircrack-ng.org/. Last visited 2010-05-30.

[52] Lucafa. 2010. Lucafa's tutorial: softap with internet connection and mitm sniffing. http://www.backtrack-linux.org/forums/beginners-forum/1939-lucafas-tutorial-softap-internet-connection-mitm-sniffing-2.html. Last visited 2010-05-20.

[53] KDE developers. 2009. KDE Kiosk framework README. http://websvn.kde.org/trunk/KDE/kdelibs/kdecore/doc/README.kiosk?view=markup. Last visited 2010-05-03.

[54] VMWare. Vmware workstation. http://www.vmware.com/products/workstation/. Last visited 2010-05-29.

[55] Bellard, F. Qemu - open source processor emulator. http://www.qemu.org. Last visited 2010-05-29.

[56] Neuman, B. & Ts'o, T. sep 1994. Kerberos: an authentication service for computer networks. *Communications Magazine, IEEE*, 32(9), 33 – 38.

[57] Neuman, C., Yu, T., Hartman, S., & Raeburn, K. July 2005. The Kerberos Network Authentication Service (V5). RFC 4120 (Proposed Standard). Updated by RFCs 4537, 5021.

[58] OpenLDAP. Openldap official home page. http://www.openldap.org/. Last visited 2010-05-30.

[59] Shamir, A. 1979. How to share a secret. *Communications of the ACM*, 22(11), 612–613.

[60] Geier, J. *Port-Based Authentication Concepts*, chapter 2.

[61] Zeuthen, D. 2007. Policykit library reference manual. http://hal.freedesktop.org/docs/PolicyKit/. Last visited 2010-05-20.

[62] Nassar, P., Badr, Y., Barbar, K., & Biennier, F. july 2009. Towards integrating security services in e-learning platforms. In *Advances in Computational Tools for Engineering Applications, 2009. ACTEA '09. International Conference on*, 573 –577.

[63] Ubuntu. 2007. Uncomplicatedfirewall. https://wiki.ubuntu.com/UncomplicatedFirewall. Last visited 2010-05-20.

[64] Golloway, J. 2006. Can operating systems tell if they're running in a virtual machine? http://weblogs.asp.net/jgalloway/archive/2006/10/27/Can-Operating-Systems-tell-if-they_2700_re-running-in-a-Virtual-Machine_3F00_.aspx. Last visited 2010-05-25.

[65] Armstrong, B. 2005. Detecting microsoft virtual machines. http://blogs.msdn.com/b/virtual_pc_guy/archive/2005/10/27/484479.aspx. Last visited 2010-05-25.

[66] Hintz, A. & Walters, A. 2004. Vmware not the perfect sandbox. http://www.securiteam.com/securitynews/5OP0B1PCAA.html. Last visited 2010-05-26.

[67] Rutkowska, J. 2006. Subverting vista kernel for fun and profit. http://blackhat.com/presentations/bh-usa-06/BH-US-06-Rutkowska.pdf. Last visited 2010-05-31.

[68] Adams, K. 2 2007. Microsoft swallows the bluepill. http://x86vmm.blogspot.com/2007/02/microsoft-swallows-bluepill.html. Last visited 2010-05-31.

[69] Adams, K. 7 2007. Bluepill detection in two easy steps. http://x86vmm.blogspot.com/2007/07/bluepill-detection-in-two-easy-steps.html. Last visited 2010-05-31.

[70] Liguori, A. 8 2006. Debunking blue pill myth. http://www.virtualization.info/2006/08/debunking-blue-pill-myth.html. Last visited 2010-05-31.

A Questionnaire

1. Har din/dine skoler holdt eksamen på PC?
   1. □ Ja
   2. □ Nei
2. I hvilket fylke ligger din skole?

   1. □Akershus
   2. □Aust-Agder
   3. □Buskerud
   4. □Finnmark
   5. □Hedmark
   6. □Hordaland
   7. □Møre og Romsdal
   8. □Nordland
   9. □Nord-Trøndelag
   10. □Oppland
   11. □Oslo
   12. □Rogaland
   13. □Sogn og Fjordane
   14. □Sør-Trøndelag
   15. □Telemark
   16. □Troms
   17. □Vest-Agder
   18. □Vestfold
   19. □Østfold

3. Hvor mange elever utgjør din/dine skoler?
   1. □ 1-50
   2. □51-100
   3. □101-200
   4. □201-300
   5. □301-400
   6. □401-500
   7. □501-600
   8. □601-700
   9. □Over 700

4. Kan IKT-basert eksamen gjennomføres på elevens egen PC? Dvs. på en maskin hvor eleven har administratortilgang og ellers alle rettigheter.

    1. □Ja
    2. □Nei, kun skolens stasjonære brukes
    3. □Nei, kun skolens bærbare brukes

5. Er det ønskelig å ta i bruk slik eksamensform?[1]
    1. □ Ja
    2. □ Nei
    3. □ Delte meninger ved skolen

6. Hvis Internett/Intranett er nødvendig under eksamen, er tilgangen gjennom trådløst eller kablet nettverk?
    1. □ Trådløst
    2. □ Kablet
    3. □ Ingen eksamen gjennomføres med nettilgang
    4. □ Annet, spesifiser her

7. Med hvilke virkemidler blir elevenes identitet verifisert?
    1. □ Tradisjonell identifisering
    2. □ Brukernavn og passord på eksamenssystem
    3. □ Begge
    4. □ Annet, spesifiser her

8. Hvordan sikres tilgjengelighet av systemene som brukes under eksamen?
    1. □ Alternative trådløse aksesspunkt settes opp ved eksamen
    2. □ Annet tiltak for redundant nettilgang
    3. □ Redundante eksamenssystemer
    4. □ Ingen tiltak
    5. □ Annet, spesifiser her

9. Hvordan sikres gjennomføringen av eksamen mot juks fra kandidatene?
    1. □ Manuell inspeksjon fra eksamensvakter
    2. □ Manuell inspeksjon fra kyndig IT-personell
    3. □ Støtte for blåtann er avslått
    4. □ Støtte for eksterne minneenheter er sperret
    5. □ Nettilgang er begrenset til skolenett
    6. □ Annet, spesifiser her

10. Hvordan sikres det mot dokumenttap av eksamensdokumenter?

[1] Ble kun stilt til de som svarte Nei på første spørsmål

1. □ Eleven må selv sørge for jevnlig backup/lagring
2. □ Systemet lagrer dokumenter automatisk med et visst intervall
3. □ Ingen tiltak
4. □ Annet, spesifiser her

11. Hvilke alternative eksamensgjennomføringsmetoder blir brukt om systemet går ned eller ikke kan brukes?
    1. □ Tradisjonell eksamensform som backup
    2. □ Annet eksamenssystem som backup
    3. □ Intet tiltak for dette
    4. □ Annet, spesifiser her

12. Fins det andre tiltak mot juks eller sabotasje fra elevens side?
13. Hvordan sikres konfidensialiteten til eksamensspørsmål og svar?
    1. □ Ingen tiltak
    2. □ Kryptering blir tatt i bruk
    3. □ Annet, spesifiser her

14. Hvordan sikres integriteten til eksamensspørsmål og svar?
    1. □ Ingen tiltak
    2. □ Digitale signaturer blir brukt
    3. □ Sikres med filadgang til kun autorisert personell (sensor,administrator etc.)
    4. □ Annet, spesifiser her

15. Hvor mange tilfeller av juks har blitt oppdaget per år?
    1. □ Ingen
    2. □ 1-3
    3. □ 4-6
    4. □ 7-9
    5. □ 10 eller mer

16. På hvilken måte har det blitt jukset under IKT-basert eksamen?
17. Hvordan unngås uønsket elektronisk kommunikasjon mellom eksamenskandidatene?
    1. □ Begrenset nettilgang med brannmur
    2. □ Begrenset nettilgang med eget program (WebSense etc.)
    3. □ Ingen nettilgang
    4. □ Bruk av blåtann er sperret
    5. □ Bruk av ikke-godkjente trådløse nettverk er sperret
    6. □ Bruk av mobile modem er sperret
    7. □ Annet, spesifiser her

18. Hvordan sikres ikke-benekting av eksamenssvar? Ikke-benekting her innebærer at elevene

kan ikke nekte for å ha levert en besvarelse hvis de faktisk har gjort det.

19. Hvilke lokale applikasjoner har eleven tilgang til under eksamen?
    1. □ Alle applikasjoner
    2. □ Alle applikasjoner foruten oversettelsesprogram i fremmedspråk
    3. □ Kun nødvendig programvare for å få gjennomført eksamen (tekstbehandling, kalkulator etc.)
    4. □ Annet, spesifiser her

20. Hvilke sikkerhetsutfordringer mener du blir taklet dårlig med dagens system?
    1. □ Vanskelig å kontrollere grunnet ukyndig personell under eksamen
    2. □ Vanskelig å hindre kommunikasjon
    3. □ Vanskelig å hindre bruk av eksterne ressurser
    4. □ Vanskelig å hindre bruk av lokale ressurser
    5. □ Annet, spesifiser her

21. I hvilken grad overvåkes eksamenskandidatene?
    1. □ Ingen overvåking
    2. □ I liten grad (noe monitorering av aktivitet)
    3. □ I middels grad
    4. □ I høy grad (mer eller mindre all aktivitet blir overvåket)

B Survey result summary

Table 27: Survey result summary

Question	Alternative	Count	Percent
1.		118	
	1	105	89.0 %
	2	13	11.0 %
2.		117	
	1	9	7.7 %
	2	3	2.6 %
	3	4	3.4 %
	4	3	2.6 %
	5	5	4.3 %
	6	8	6.8 %
	7	12	10.3 %
	8	6	5.1 %
	9	7	6.0 %
	10	2	1.7 %
	11	8	6.8 %
	12	3	2.6 %
	13	7	6.0 %
	14	13	11.1 %
	15	3	2.6 %
	16	9	7.7 %
	17	6	5.1 %
	18	5	4.3 %
	19	4	3.4 %
3.		116	
	1	2	1.7 %
	2	3	2.6 %
	3	20	17.2 %
	4	14	12.1 %
	5	12	10.3 %
	6	19	16.4 %
	7	14	12.1 %
	8	13	11.2 %

Table 27: Survey result summary

Question	Alternative	Count	Percent
	9	19	16.4 %
4.		103	
	1	50	48.5 %
	2	20	19.4 %
	3	33	32.0 %
5.		13	
	1	9	69.2 %
	2	1	7.7 %
	3	3	23.1 %
6.		103	
	1	69	67.0 %
	2	14	13.6 %
	3	8	7.8 %
	4	12	11.7 %
7.		102	
	1	23	22.5 %
	2	36	35.3 %
	3	37	36.3 %
	4	6	5.9 %
8.		102	
	1	9	8.8 %
	2	26	25.5 %
	3	10	9.8 %
	4	38	37.3 %
	5	33	32.4 %
9.		103	
	1	67	65.0 %
	2	47	45.6 %
	3	43	41.7 %
	4	15	14.6 %
	5	56	54.4 %
	6	35	34.0 %

Table 27: Survey result summary

Question	Alternative	Count	Percent
10.		103	
	1	74	71.8 %
	2	19	18.4 %
	3	1	1.0 %
	4	9	8.7 %
11.		103	
	1	66	64.1 %
	2	9	8.7 %
	3	12	11.7 %
	4	16	15.5 %
13.		102	
	1	56	54.9 %
	2	24	23.5 %
	3	22	21.6 %
14.		100	
	1	30	30.0 %
	2	5	5.0 %
	3	61	61.0 %
	4	11	11.0 %
15.		99	
	1	69	69.7 %
	2	24	24.2 %
	3	4	4.0 %
	4	0	0.0 %
	5	2	2.0 %
17.		102	
	1	53	52.0 %
	2	28	27.5 %
	3	22	21.6 %
	4	40	39.2 %
	5	33	32.4 %
	6	28	27.5 %

Table 27: Survey result summary

Question	Alternative	Count	Percent
	7	20	19.6 %
19.		103	
	1	54	52.4 %
	2	20	19.4 %
	3	24	23.3 %
	4	5	4.9 %
20.		96	
	1	66	68.8 %
	2	59	61.5 %
	3	34	35.4 %
	4	30	31.3 %
	5	18	18.8 %
21.		103	
	1	14	13.6 %
	2	45	43.7 %
	3	31	30.1 %
	4	13	12.6 %

C Adapted assessment framework

Table 28: Table with assessment overview

Security catalogue of criteria			
Security pillar	ID	Value	Security service
Availability	1.1	[0.3]	Distributed architecture
	1.2	[0.8]	Automatic fallback-system
	1.3	[0.7]	Regular backup ensured by system
Non-repudiation	2.1	[0.7]	Ensured with digital signatures
	2.2	[0.6]	Ensured with OTP token
	2.3	[0.2]	Ensured by external system
Integrity	3.1	[0.8]	Exam content is digitally signed
	3.2	[0.6]	Message Authentication Codes are used for exam content
	3.3	[0.8]	Distributed architecture with write protection
	3.4	[0.7]	Security policy models (Biba, Clark Wilson etc.)
	3.5	[0.7]	Operating system integrity is preserved
	3.6	[0.5]	Intrusion detection mechanism implemented in system to detect privilege escalation or other malicious activity
Confidentiality	4.1	[0.8]	Encryption of information in transit(symmetric/asymmetric)
	4.2	[0.6]	Security policy models implemented (e.g. Bell-La Padula)
	4.3	[0.6]	Encryption of stored exam content
Authorization	5.1	[0.7]	Access to Internet is restricted/limited by examination system
	5.2	[0.7]	Access with Bluetooth/IR to other devices or networks are completely disabled
	5.3	[0.7]	Access to Internet is restricted/limited with a firewall
	5.4	[0.6]	Access to rogue access points are prohibited
	5.5	[0.7]	Access to internal hard drive is prohibited
	5.6	[0.6]	Access to external hard drives are prohibited
	5.7	[0.5]	Security mechanisms of system cannot be circumvented by crash
	5.8	[0.6]	Security mechanisms of system cannot be circumvented by running the system in a virtual machine
	5.8.1	[0.5]	Secured by implementing technical security measures to prevent circumvention
	5.8.2	[0.4]	Secured by implementing procedural security measures to prevent circumvention

Table 28: Table with assessment overview

Security catalogue of criteria			
Security pillar	ID	Value	Security service
Authentication	6.1	[0.1]	Password based authentication
	6.1.1	[0.2]	Every user has their own account (no group accounts)
	6.1.2	[0.2]	Authentication of physical users with ID possible
	6.1.3	[0.7]	Password are checked for strength against dictionaries or with other analysis
	6.1.4	[0.7]	Passwords are encrypted in transit and when stored
	6.1.5	[0.4]	Access control for password file
	6.1.6	[0.2]	Frequent password changing
	6.2	[0.1]	Token based authentication
	6.3	[0.2]	Biometric authentication
	6.3.1	[0.8]	Life detection
	6.3.2	[0.6]	Skin resistance
	6.3.3	[0.8]	High resolution images are used
	6.4	[0.1]	Multiple logins prohibited
	6.5	[0.5]	Replay attacks prohibited
	6.6	[0.2]	Message about last login
	6.7	[0.5]	Exam content only accessible with dual authentication (one for student and one for invigilator/system administrator)

D Proof-of-concept code to detect presence of VMWare

```
/*
** Not written by thesis author, however modified to     **
** work under Ubuntu 9.04 with GCC version 4.3.3    -Petter **
*
* 4tphi-vmchk.c
* Detects if you are in a VMWare virtual machine.
*
* Written by Andrew Hintz and AAron Walters
* Fortify Research Laboratories
*
* This program is based on info and code from:
* http://chitchat.tripod.co.jp/vmware/
* by chitchat@lycos.jp
*
* Notes:
* The program can be run as a normal user. We tested the program
* only in x86 Linux. The m4dn3ss lives on!
*/

#include  <stdio.h>
#include  <stdlib.h>
#include  <signal.h>


#if __INTSIZE == 2 /* 16 bit environment */
typedef unsigned int uint16;
typedef unsigned long uint32;
#else /* 32 bit environment */
typedef unsigned short uint16;
typedef unsigned int uint32;
#endif /* __INTSIZE */

void segfault(){
printf("Not running inside VMware.\n");
exit(1);
}

int main(){
uint32 verMajor, verMinor, magic, dout;

signal(SIGSEGV, segfault);

__asm__ __volatile__ (
"mov $0x564D5868, %%eax;" /* magic number */
"mov $0x3c6cf712, %%ebx;" /* random number */
"mov $0x0000000A, %%ecx;" /* specifies command */
"mov $0x5658, %%edx;" /* VMware I/O port */

"in %%dx, %%eax;"

"mov %%eax, %0;"
"mov %%ebx, %1;"
"mov %%ecx, %2;"
```

```
54 "mov %%edx, %3;"
55
56 : "=r"(verMajor), "=r"(magic), "=r"(verMinor), "=r"(dout)
57 );
58
59 if (magic == 0x564D5868) {
60 printf("Running inside VMware. ");
61 printf("(Version %i,%i)\n", verMajor, verMinor);
62 /* I'm not really sure what the versions mean. */
63 }
64
65 return 0;
66
67 }/* end main */
68
69 /* end of file */
```

Listing D.1: Proof-of-concept code to detect the VMWare host

E Extended assessment

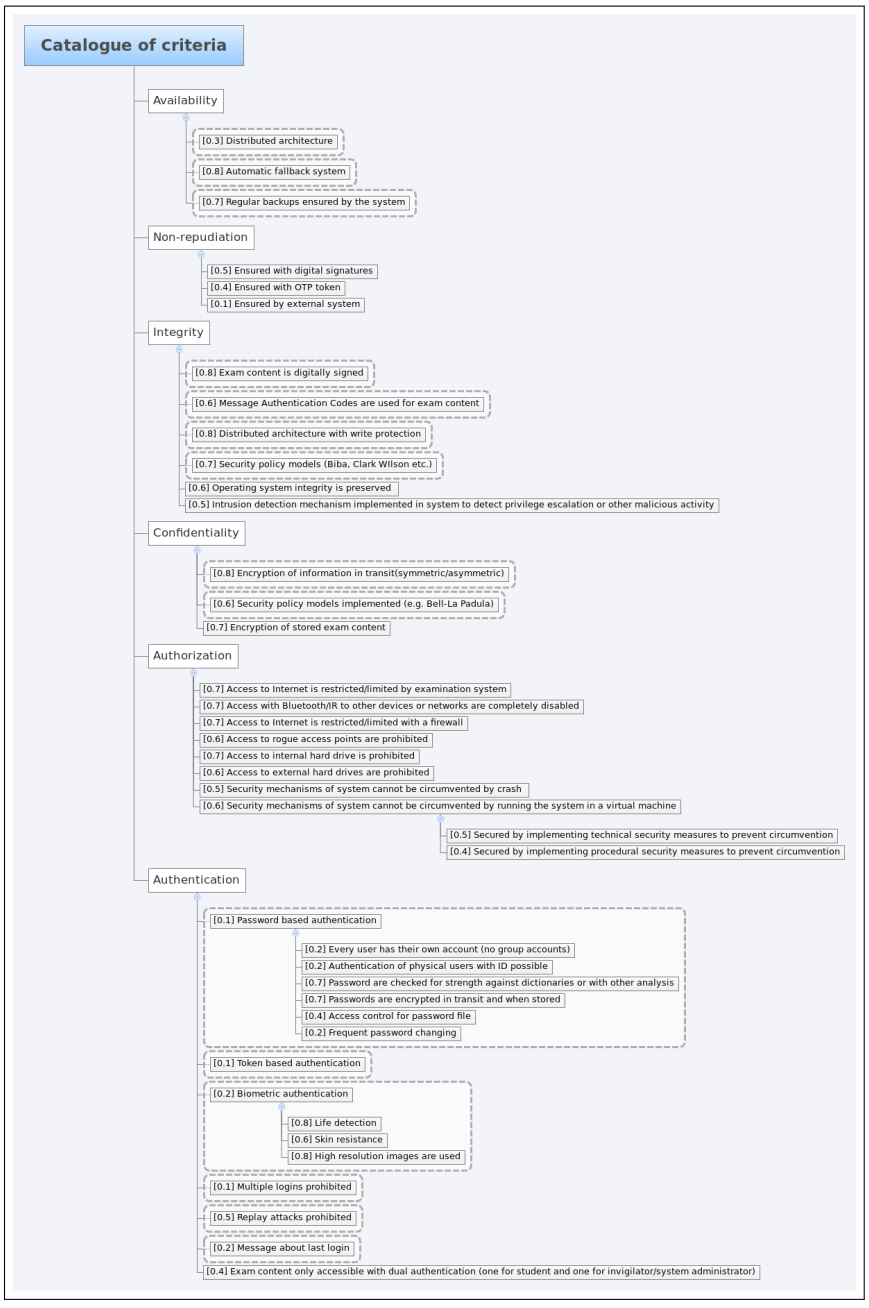


Figure 32: Adopted catalogue of criteria

F Security testing of examination systems

F.1 Availability

1.1 The exam system consists of a distributed architecture
Identify the elements of the architecture. Are all elements documented? Remember to include all identified elements in later tests.
Score: **0**□ **1**□ **2**□ **3**□points
Comments:
_____
_____
_____

1.2 The exam system has an automatic fallback system
If Yes:
This is a procedural measure and cannot tested extensively with technical means.
Score: **0**□ **1**□ **2**□ **3**□points
Comments:
_____
_____
_____

1.3 Regular backups are ensured by the system
If Yes:
Create a new document without saving it. Write three paragraphs of placeholder text, note how many words that are written. Simulate a crash by turning off the computer with the use of the power button. Turn the computer on and see how much of the document that are recovered.
If nothing is recovered, do the same test again but this time with saving it before writing any text.
Score: **0**□ **1**□ **2**□ **3**□points
Comments:
_____
_____
_____

F.2 Non-repudiation

2.1 Non-repudiation is ensured with digital signatures
If yes:
How are these signatures generated? Are the private keys stored securely? How? (E.G. Smart card)
Score: **0**□ **1**□ **2**□ **3**□points
Comments:
_____
_____
_____

2.2 Non-repudiation is ensured with one-time password token
If Yes: How are the token managed? Can the system be spoofed by just handing over the token to another person?
Score: **0**□ **1**□ **2**□ **3**□points
Comments:
_____
_____
_____

2.3 Ensured by external system
If Yes:
Testing of external systems is outside of the scope of this testing scheme.
Score: **0**□ **1**□ **2**□ **3**□points
Comments:
_____
_____
_____

F.3 Integrity

3.1 Exam content is digitally signed
If Yes:
See 2.1
Score: **0**□ **1**□ **2**□ **3**□points
Comments:
_____
_____
_____

3.2 Message Authentication Codes are used for exam content
If Yes:
What algorithms are used? How are keys distributed? Are there any clear vulnerabilities regarding this specific implementation?
Score: **0**□ **1**□ **2**□ **3**□points
Comments:
_____
_____
_____

3.3 Distributed architecture with write protection
If Yes:
Verify the elements in the architecture. How is it implemented?
Score: **0**□ **1**□ **2**□ **3**□points
Comments:
_____
_____
_____

3.4 Security policy models (Biba, Clark Wilson etc.)
If Yes: N/A

3.5 Operating system integrity is preserved
If Yes: How is OS integrity preserved? Is there ways to circumvent these measures? Can the student use their own version of the OS/examination system to spoof a valid system?
Score: **0**□ **1**□ **2**□ **3**□points
Comments:
_____
_____
_____

3.6 Intrusion detection mechanism implemented in system to detect privilege escalation or other malicious activity
If Yes: What kind of mechanisms are implemented? Is intrusion detected real time, or will incidents only be detected after the examination is conducted?
Score: **0**□ **1**□ **2**□ **3**□points
Comments:
_____
_____
_____

F.4 Confidentiality

4.1 Encryption of information in transit(symmetric/asymmetric)
What enciphering/deciphering algorithms are used ? What is the key length used, and is this mandatory? What is the key based on (how random)? How is key-management being performed?
Score: **0**□ **1**□ **2**□ **3**□points
Comments:
_____
_____
_____

4.2 Security policy models implemented (e.g. Bell-La Padula)
N/A
Score: **0**□ **1**□ **2**□ **3**□points
Comments:
_____
_____
_____

4.3 Encryption of stored exam content
What enciphering/deciphering algorithms are used ? What is the key length used, and is this mandatory? What is the key based on (how random)? How is key-management being performed?
Score: **0**□ **1**□ **2**□ **3**□points
Comments:
_____
_____
_____

F.5 Authorization

5.1 Access to Internet is restricted/limited by examination system
What method is used to perform this limitation (blacklist/whitelist)? Is it possible to bypass the limitations in any way? (e.g. Try URL evasion techniques). Test "illegal" sites that are meant to be blocked. Test network access with other applications than browsers.
Score: **0**□ **1**□ **2**□ **3**□points
Comments:
_____
_____
_____

5.2 Access with Bluetooth/IR to other devices or networks are completely disabled
How is this implemented? If it is disabled, can it be enabled by the student in any way?
Score: **0**□ **1**□ **2**□ **3**□points
Comments:
_____
_____
_____

5.3 Access to Internet is restricted/limited with a firewall
What method is used to perform this limitation (blacklist/whitelist)? Is it possible to bypass the limitations in any way? (e.g. Try URL evasion techniques). Test "illegal" sites are blocked.
Score: **0**□ **1**□ **2**□ **3**□points
Comments:
_____
_____
_____

5.4 Access to rogue access points are prohibited
Test access to other Access Points. Is the examination student user able to connect to other APs? Is it possible to spoof the legitimate access point?
Score: **0**□ **1**□ **2**□ **3**□points
Comments:
_____
_____
_____

5.5 Access to internal hard drive is prohibited
If the internal hard drive is mounted, see if the student user has access to these files in the examination system. If it is not mounted, can it be mounted? If access is limited, but only by the means of restricting use of file explorers and terminals/shells, see if online file explorer can be used (e.g. http://ikat.ha.cked.net/).
Score: **0**□ **1**□ **2**□ **3**□points
Comments:
_____
_____
_____

5.6 Access to external hard drives are prohibited

Will a hot-plugged usb-memory stick be mounted on the system? If so, can the student access files on this device?

Score: **0**□ **1**□ **2**□ **3**□points

Comments:

_____
_____
_____

5.7 Security mechanisms of system cannot be circumvented by crash

Either inadvertently or with intention, is the student able to circumvent security measures by a crash? Force a crash (e.g. press power button), can the student boot their own operating system without being detected?

Score: **0**□ **1**□ **2**□ **3**□points

Comments:

_____
_____
_____

5.8 There are countermeasures to prevent running the system in a virtual machine

See what happens if the system is run in a virtual machine, test both Vmware and Virtualbox. Is the examination system usable in a virtual environment? (if possible test hardware virtualization)

Score: **0**□ **1**□ **2**□ **3**□points

Comments:

_____
_____
_____

5.8.1 Secured by implementing technical security measures to prevent running the system in a virtual machine

If the above test failed, it means that the technical measures to prevent this works properly. More detailed tests with different hardware/software may be performed.

Score: **0**□ **1**□ **2**□ **3**□points

Comments:

_____
_____
_____

5.8.2 Secured by implementing procedural security measures to prevent running the system in a virtual machine(e.g. visual inspection at boot time, and/or at periodic intervals during examination)

Is it possible to run it in a virtual machine, and make the boot seem legitimate?

Score: **0**□ **1**□ **2**□ **3**□points

Comments:

_____
_____
_____

F.6 Authentication

6.1 Password based authentication is used

How is this implemented? What is the password policy? Is brute-force attacks possible?

Score: **0**□ **1**□ **2**□ **3**□points

Comments:

_____
_____
_____

6.1.1 Every user has their own account (no group accounts)

Score: **0**□ **1**□ **2**□ **3**□points

Comments:

_____
_____
_____

6.1.2 Authentication of physical users with ID possible

Score: **0**□ **1**□ **2**□ **3**□points

Comments:

_____
_____
_____

6.1.3 Password are checked for strength against dictionaries or with other analysis

Verify this functionality.

Score: **0**□ **1**□ **2**□ **3**□points

Comments:

_____
_____
_____

6.1.4 Passwords are encrypted in transit and when stored

Perform network analysis while authentication with username and password, and observe if this is encrypted or not.

Score: **0**□ **1**□ **2**□ **3**□points

Comments:

_____
_____
_____

6.1.5 Access control for password file

Verify this security functionality by inspecting the access control policy for this file.

Score: **0**□ **1**□ **2**□ **3**□points

Comments:

_____
_____
_____

6.1.6 Frequent password changing

Verify the functionality regarding password policy, and look into possibilities to bypass this security measure.

Score: **0**□ **1**□ **2**□ **3**□points

Comments:

_____
_____
_____

6.2 Token based authentication (smart card, proximity device, etc.)

Is the token prone to spoofing attacks? Is it used in conjugation with something one know or are? How are these devices distributed, and what happens if the devices are lost?

Score: **0**□ **1**□ **2**□ **3**□points

Comments:

_____
_____
_____

6.3 Biometric authentication

Testing of biometric authentication is outside the scope of this master thesis

Score: **0**□ **1**□ **2**□ **3**□points

Comments:

_____
_____
_____

6.3.1 Life detection

Comments:

_____
_____
_____

6.3.2 Skin resistance

Comments:

_____
_____
_____

6.3.3 High resolution images are used

Comments:

_____
_____
_____

6.4 Multiple logins prohibited

Check if the same user can log in at the same time in two different computers.

Score: **0**□ **1**□ **2**□ **3**□points

Comments:

_____
_____
_____

6.5 Replay attacks prohibited

Look into the possibility to retransmit messages sent from student to examination system.

Score: **0**□ **1**□ **2**□ **3**□points

Comments:

_____
_____
_____

6.6 Message about last login

Verify the functionality, and look into possibilities to bypass this security measure. Can the message be spoofed?

Score: **0**□ **1**□ **2**□ **3**□points

Comments:

_____
_____
_____

6.7 Exam content only accessible with dual authentication (one for student and one for invigilator/system administrator)

Verify the functionality, and look into possibilities to bypass this security measure.

Score: **0**□ **1**□ **2**□ **3**□points

Comments:

_____
_____
_____