

# Securing ICT-based examinations

Introduction

Survey

Analysis of  
current  
solutions

Assessment

Testing

Proposed  
require-  
ments/imple-  
mentations

Conclusion

Future work

**Petter Bjørklund**



June 8, 2010

# Main outline

## Securing ICT-based examinations

Petter  
Bjørklund

### Introduction

Survey

Analysis of  
current  
solutions

Assessment  
Testing

Proposed  
require-  
ments/imple-  
mentations

Conclusion

Future work

- 1 Introduction
- 2 Survey
- 3 Analysis of current solutions
- 4 Proposed requirements/implementations
- 5 Conclusion
- 6 Future work

# Problem description

## Securing ICT-based examinations

Petter  
Bjørklund

### Introduction

Survey

Analysis of  
current  
solutions

Assessment

Testing

Proposed  
require-  
ments/imple-  
mentations

Conclusion

Future work

- Schools instructed to conduct ICT-based examinations
- Technology literate students poses a challenge to technology challenged invigilators<sup>1</sup>
- Use of illegal aids may be very tempting
- Thesis proposer Norwegian Computing Center have developed a prototype (*digeks*) of an examination system to mitigate use of illegal aids
- The prototype is based on live version of a Linux distribution booted from USB
- Increased level of security in the ICT-based examination system is desired

---

<sup>1</sup>Person responsible for "guarding" examination. [Norwegian: eksamensvakt](#) ↻ 🔍

# Motivation

## Securing ICT-based examinations

Petter  
Bjørklund

### Introduction

Survey

Analysis of  
current  
solutions

Assessment

Testing

Proposed  
require-  
ments/imple-  
mentations

Conclusion

Future work

- Important to trust the educational establishment
- Correctness of exams ensures a certain level of trust
- Misuse of trust relationship triggered by use of illegal aids

# Research questions

## Securing ICT-based examinations

Petter  
Bjørklund

### Introduction

Survey

Analysis of  
current  
solutions

Assessment  
Testing

Proposed  
require-  
ments/imple-  
mentations

Conclusion

Future work

- 1 What is the best practice of ICT-based examination security in educational institutions today?

# Research questions

## Securing ICT-based examinations

Petter  
Bjørklund

### Introduction

Survey

Analysis of  
current  
solutions

Assessment

Testing

Proposed  
require-  
ments/imple-  
mentations

Conclusion

Future work

- 1 What is the best practice of ICT-based examination security in educational institutions today?
  - Investigate current security situation in Norwegian high schools
  - In order to increase a current level of security, a method for assessing this level must be found
  - Assessment of current solutions will give indications on focus areas of security

# Research questions cont.

## Securing ICT-based examinations

Petter  
Bjørklund

### Introduction

Survey

Analysis of  
current  
solutions

Assessment

Testing

Proposed  
require-  
ments/imple-  
mentations

Conclusion

Future work

- 2 What are the prioritized security requirements for conducting ICT-based exams?

# Research questions cont.

## Securing ICT-based examinations

Petter  
Bjørklund

### Introduction

Survey

Analysis of  
current  
solutions

Assessment  
Testing

Proposed  
require-  
ments/imple-  
mentations

Conclusion

Future work

- 2 What are the prioritized security requirements for conducting ICT-based exams?
  - Testing will lead to confirmation or invalidation of implemented security measures
  - A collection of security requirements will be the product of the testing phase

# Research questions cont.

## Securing ICT-based examinations

Petter  
Bjørklund

### Introduction

Survey

Analysis of  
current  
solutions

Assessment

Testing

Proposed  
require-  
ments/imple-  
mentations

Conclusion

Future work

- 
- 
- 3 What security measures and protocols need to be implemented to adhere to these requirements?

# Research questions cont.

## Securing ICT-based examinations

Petter  
Bjørklund

### Introduction

Survey

Analysis of  
current  
solutions

Assessment

Testing

Proposed  
require-  
ments/imple-  
mentations

Conclusion

Future work

- 3 What security measures and protocols need to be implemented to adhere to these requirements?
  - Each of the requirements might or might not have applicable implementation possibilities
  - Security measures will be proposed to cover the requirements presented

# Survey preparation

## Securing ICT-based examinations

Petter  
Bjørklund

Introduction

**Survey**

Analysis of  
current  
solutions

Assessment  
Testing

Proposed  
require-  
ments/imple-  
mentations

Conclusion

Future work

- Investigate the best practice conveyed by Norwegian high schools focusing on security
- System administrator at these schools considered to be the most suitable subjects
- 446 high schools in Norway<sup>2</sup>
- Contact information for 405 schools were collected
- Invitation to participate in the survey were sent out to all of these schools
- 118 system administrators participated

---

<sup>2</sup>School year of 2008/2009

# Survey results

## Securing ICT-based examinations

Petter Bjørklund

Introduction

**Survey**

Analysis of current solutions

Assessment

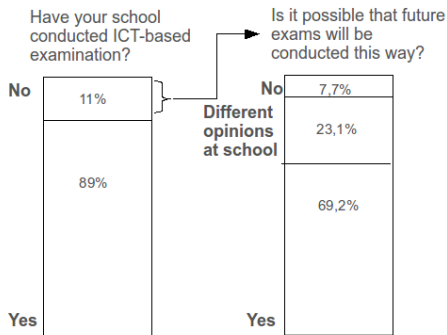
Testing

Proposed requirements/implementations

Conclusion

Future work

- 9 out of 10 schools have already conducted ICT-based examinations
- 1 out of 118 schools have not and will not conduct ICT-based examinations



# Survey results cont.

## Securing ICT-based examinations

Petter  
Bjørklund

Introduction

**Survey**

Analysis of  
current  
solutions

Assessment

Testing

Proposed  
require-  
ments/imple-  
mentations

Conclusion

Future work

- Almost half of the schools permit the students to use their own computer
- Half of the schools allows all applications during the exam
- 92,2% of schools have network access enabled during examinations
- Invigilators are the most used remedy for cheating mitigation
- Invigilators are also seemed as the biggest security challenge
- Another big challenge is blocking communication
- 7 out of 10 schools does not report any cheating incidents
- 2 out of 1000 students are reported for cheating per year
- There are varying policies regarding surveillance of students

# Survey results cont.

- Assumption of proportional increase in reported incidents based on the level of surveillance prior to survey

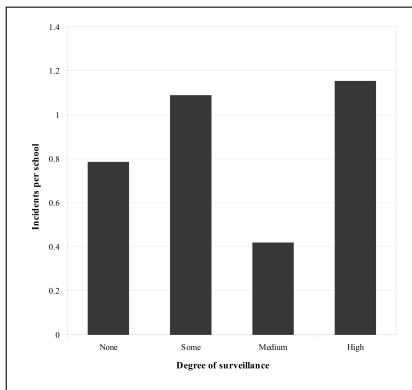


Figure: Surveillance degree and incidents

# Survey results cont.

## Securing ICT-based examinations

Petter  
Bjørklund

Introduction

Survey

Analysis of  
current  
solutions

Assessment

Testing

Proposed  
require-  
ments/imple-  
mentations

Conclusion

Future work

- Some observations based on survey:
  - Schools with school controlled computers are more inclined to report incidents than schools that permit students to bring their own computer
  - Schools with student controlled computers are more inclined to use wireless network access
  - Application policy is not influenced by what kind of computer is used

# Analysing current solutions

## Securing ICT-based examinations

Petter  
Bjørklund

Introduction

Survey

**Analysis of  
current  
solutions**

Assessment

Testing

Proposed  
require-  
ments/imple-  
mentations

Conclusion

Future work

- In addition to *digeks*, one examination system were chosen for assessment and testing
- Australia-based *eExam* is also based on a live version of a Linux based operating system
  - Thus, both systems can be used with students own laptop
- Both systems are freely available for use and documentation is also publicly available

# Method of assessment

## Securing ICT-based examinations

Petter  
Bjørklund

Introduction

Survey

Analysis of  
current  
solutions

**Assessment**

Testing

Proposed  
require-  
ments/imple-  
mentations

Conclusion

Future work

- Related work identified existing framework for assessing security in e-learning systems
- A modified version of this framework were adopted
- It included security services from the examination setting

# Method of assessment cont.

## Securing ICT-based examinations

Petter  
Bjørklund

Introduction

Survey

Analysis of  
current  
solutions

**Assessment**

Testing

Proposed  
require-  
ments/imple-  
mentations

Conclusion

Future work

- The framework consists of six main security categories
  - Authentication
  - Availability
  - Non-Repudiation
  - Integrity
  - Confidentiality
  - Authorization
- Each category consists of several security services
- Each service is rated within the open interval of  $(0,1)$
- A security rating for each category is calculated and the overall assessment score is the arithmetic mean of these ratings

# Assessment results

- A self-assessment form were sent out to key personnel connected to the development of *eExam* and *digeks*
- The results are based on their responses

**Table:** Assessment applied for the 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
<b>Overall score</b>	<b>0.199</b>

(b) Scores for digeks

Authentication	0.100
Availability	0.790
Non-Repudiation	0.000
Integrity	0.000
Confidentiality	0.000
Authorization	0.994
<b>Overall score</b>	<b>0.314</b>

# Testing method

- The objective of the testing is to investigate the reported implemented security measures
- A score system were developed to give scores to each measure based on test findings
  - Example: One major weakness in System A leads to possibility for covert channel attack: Score 1/3.
- The arithmetic mean of these scores gives us the total coverage degree of a system

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

# Testing results

Table: Testing result table

System	# services reported	Coverage degree
eExam	7	76,19%
digeks	8	79,17%

Some vulnerabilities revealed in the testing phase:

- eExam:
  - Unauthorized file access vulnerability
  - Spoofing vulnerability
- Digeks:
  - DoS-vulnerability
  - Covert channel vulnerability

# Requirement and implementation possibility

## Securing ICT-based examinations

Petter  
Bjørklund

Introduction

Survey

Analysis of  
current  
solutions

Assessment  
Testing

**Proposed  
require-  
ments/imple-  
mentations**

Conclusion

Future work

- Several requirements are defined based on findings in assessment and testing
- Implementation possibilities are also presented as a starting point to adhere to these requirements

# Conclusion

## Securing ICT-based examinations

Petter  
Bjørklund

Introduction

Survey

Analysis of  
current  
solutions

Assessment

Testing

Proposed  
require-  
ments/imple-  
mentations

**Conclusion**

Future work

- A good overview of how security is conceived and handled at the high schools have been the result of the survey
- Current solutions are assessed and tested
  - Opens for assessment and testing as a repetitive task in the future
  - The combined method of assessment and testing can be used in other settings as well
- A set of requirements are found based on testing and these have opened for implementation possibilities

# Future work

## Securing ICT-based examinations

Petter  
Bjørklund

Introduction

Survey

Analysis of  
current  
solutions

Assessment

Testing

Proposed  
require-  
ments/imple-  
mentations

Conclusion

Future work

- Improving method for assessment and testing
  - Weighting of the categories
  - Re-evaluate values of security services in assessment
- Implement security features based on the proposed requirements
- Perform uncertainty study regarding cheating among students. Before and after new implementation.

# The end

## Securing ICT-based examinations

Petter  
Bjørklund

Introduction

Survey

Analysis of  
current  
solutions

Assessment

Testing

Proposed  
require-  
ments/imple-  
mentations

Conclusion

**Future work**

Thank you for your attention. Time for questions!

# Method of assessment cont.

## Securing ICT-based examinations

Petter  
Bjørklund

Introduction

Survey

Analysis of  
current  
solutions

Assessment

Testing

Proposed  
require-  
ments/imple-  
mentations

Conclusion

Future work

## Security category rating (based on assessment framework by Weibl)

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

Where  $n(i)$  is the number of security services considered for category number  $i$ . The security service value  $q_{i,j}$  is in the open interval  $(0, 1)$  and  $r_{i,j}$  is the relevance parameter of each service. The relevance parameter is used to describe if the service is applicable for the evaluated system and  $r_{i,j} \in \{0, 1\}$ .