Formal Analysis of Electronic Exams

Jannik Dreier\textsuperscript{1}, Rosario Giustolisi\textsuperscript{2}, Ali Kassem\textsuperscript{3}, Pascal Lafourcade\textsuperscript{4}, Gabriele Lenzini\textsuperscript{2} and Peter Y. A. Ryan\textsuperscript{2}

\textsuperscript{1}Institute of Information Security, ETH Zurich
\textsuperscript{2}SnT/University of Luxembourg
\textsuperscript{3}Université Grenoble Alpes, CNRS, VERIMAG
\textsuperscript{4}University d’Auvergne, LIMOS

1\textsuperscript{st} Symposium on Digital Trust in Auvergne
Clermont-Ferrand, France

December 4, 2014
Electronic Exams

Coursera

Udacity

edX

IELTS

Cisco CCNA

TOEFL iBT
E-exam: Players and Organization

Three Roles:

Candidate  Examination Authority  Examiner
E-exam: Players and Organization

Three Roles:

Candidate | Examination Authority | Examiner

Four Phases:

Threats...

- Candidate cheating
- Bribed, corrupted or unfair examiners
- Dishonest/untrusted exam authority
- Outside attackers
- ...
Most existing e-exam systems assume trusted authorities and focus on student cheating:

- Exam centers
- Software solutions, e.g. ProctorU
Most existing e-exam systems assume trusted authorities and focus on student cheating:

- Exam centers
- Software solutions, e.g. ProctorU

Yet also the other threats are real:
- Atlanta Public Schools scandal (2009)
- UK student visa tests fraud (2014)
Most existing e-exam systems assume trusted authorities and focus on student cheating:

- Exam centers
- Software solutions, e.g. ProctorU

Yet also the other threats are real:
- Atlanta Public Schools scandal (2009)
- UK student visa tests fraud (2014)

So what about dishonest authorities or hackers attacking the system?
Most existing e-exam systems assume trusted authorities and focus on student cheating:

- Exam centers

- Software solutions, e.g. ProctorU

Yet also the other threats are real:

- Atlanta Public Schools scandal (2009)
- UK student visa tests fraud (2014)

So what about dishonest authorities or hackers attacking the system?

⇒ need for better protocols and systems (cf. case studies)
Most existing e-exam systems assume trusted authorities and focus on student cheating:

- Exam centers

- Software solutions, e.g. ProctorU

Yet also the other threats are real:

- Atlanta Public Schools scandal (2009)
- UK student visa tests fraud (2014)

So what about dishonest authorities or hackers attacking the system?

⇒ need for better protocols and systems (cf. case studies)
⇒ precise formal definitions of required properties
The model involves:

- **Processes** in the applied $\pi$-calculus [AF01]
- Annotated using **events**
- **Authentication** properties as **correspondence** between events
- **Privacy** properties as **observational equivalence** between instances
- **Automatic** verification using ProVerif [Bla01]
Authentication and Integrity Properties

- **Answer Origin Authentication**: All collected answers originate from registered candidates, and only one answer per candidate is accepted.
- **Form Authorship**: Answers are collected as submitted, i.e. without modification.
- **Form Authenticity**: Answers are marked as collected.
- **Mark Authenticity**: The candidate is notified with the mark associated to his answer.
Answer Origin Authentication

All collected answers originate from registered candidates, and only one answer per candidate is accepted.

Definition:
Answer Origin Authentication

All collected answers originate from registered candidates, and only one answer per candidate is accepted.

**Definition:**

On every trace:

1. Registration

2. Examination

Register

Questions

\[\text{reg}(\text{candidate})\]

\[\text{collected}(\text{candidate}, ?, !)\]

preceeded by distinct occurrence
Privacy Properties

- **Question Indistinguishability**: No premature information about the questions is leaked.
- **Anonymous Marking**: An examiner cannot link an answer to a candidate.
- **Anonymous Examiner**: A candidate cannot know which examiner graded his copy.
- **Mark Privacy**: Marks are private.
- **Mark Anonymity**: Marks are published, but not linked to candidates. Implied by Mark Privacy.
Anonymous Marking

An examiner cannot link an answer to a candidate.

Definition:

Up to the end of marking phase:

Exam 1

- Answer 1
- Answer 2

Exam 2

- Answer 2
- Answer 1

Can be considered with or without dishonest examiners and authorities.
Anonymous Marking

An examiner cannot link an answer to a candidate.

Definition:

Up to the end of marking phase:

Exam 1

Answer 1

Answer 2

≈

Exam 2

Answer 2

Answer 1

Can be considered with or without dishonest examiners and authorities.
Application: Huszti & Pethő’s Protocol

“A Secure Electronic Exam System” [HP10] using

- ElGamal Encryption
- a Reusable Anonymous Return Channel (RARC) [GJ03]

Formal Verification with ProVerif [Bla01]:

<table>
<thead>
<tr>
<th>Property</th>
<th>Result</th>
<th>Time</th>
</tr>
</thead>
<tbody>
<tr>
<td>Answer Origin Authentication</td>
<td>✗</td>
<td>&lt; 1 s</td>
</tr>
<tr>
<td>Form Authorship</td>
<td>✗</td>
<td>&lt; 1 s</td>
</tr>
<tr>
<td>Form Authenticity</td>
<td>✗</td>
<td>&lt; 1 s</td>
</tr>
<tr>
<td>Mark Authenticity</td>
<td>✗</td>
<td>&lt; 1 s</td>
</tr>
<tr>
<td>Question Indistinguishability</td>
<td>✗</td>
<td>&lt; 1 s</td>
</tr>
<tr>
<td>Anonymous Marking</td>
<td>✗</td>
<td>8 m 46 s</td>
</tr>
<tr>
<td>Anonymous Examiner</td>
<td>✗</td>
<td>9 m 8 s</td>
</tr>
<tr>
<td>Mark Privacy</td>
<td>✗</td>
<td>39 m 8 s</td>
</tr>
<tr>
<td>Mark Anonymity</td>
<td>✗</td>
<td>1h 15 m 58 s</td>
</tr>
</tbody>
</table>
A recent protocol [GLR14] using
- an exponentiation mixnet [HS11] to create pseudonyms from the parties’ public keys, to encrypt and sign anonymously
- a public append-only bulletin board

Formal Verification with ProVerif:

<table>
<thead>
<tr>
<th>Property</th>
<th>Result</th>
<th>Time</th>
</tr>
</thead>
<tbody>
<tr>
<td>Answer Origin Authentication</td>
<td>✓</td>
<td>&lt; 1 s</td>
</tr>
<tr>
<td>Form Authorship</td>
<td>✓</td>
<td>&lt; 1 s</td>
</tr>
<tr>
<td>Form Authenticity</td>
<td>✓¹</td>
<td>&lt; 1 s</td>
</tr>
<tr>
<td>Mark Authenticity</td>
<td>✓</td>
<td>&lt; 1 s</td>
</tr>
<tr>
<td>Question Indistinguishability</td>
<td>✓</td>
<td>&lt; 1 s</td>
</tr>
<tr>
<td>Anonymous Marking</td>
<td>✓</td>
<td>2 s</td>
</tr>
<tr>
<td>Anonymous Examiner</td>
<td>✓</td>
<td>1 s</td>
</tr>
<tr>
<td>Mark Privacy</td>
<td>✓</td>
<td>3 m 32 s</td>
</tr>
<tr>
<td>Mark Anonymity</td>
<td>✓</td>
<td>2³</td>
</tr>
</tbody>
</table>

¹after fix
²implied by Mark Privacy
Conclusion

- **E-exams** are used and vulnerable to attacks
- Cryptographic protocols exist, but lack **formal verification**
- **First formal framework** for analysis of e-exams:
  - Formal model in the **applied π-calculus**
  - **Definitions** for central authentication, integrity and privacy properties
- **Automated verification in ProVerif** of two case studies:
  - Huszti & Pethő’s protocol: Fails on all properties due to severe flaws in protocol design
  - Remark! protocol: Ensures all properties after one fix
- **Future work**:
  - enforced privacy
  - verifiability and accountability
  - analyzing implementations
Thank you for your attention!

Questions?

jannik.dreier@inf.ethz.ch

M. Abadi and C. Fournet.
Mobile values, new names, and secure communication.

Bruno Blanchet.
An efficient cryptographic protocol verifier based on prolog rules.

P. Golle and M. Jakobsson.
Reusable anonymous return channels.

Remark!: A secure protocol for remote exams.
to appear. Draft

A. Huszti and A. Pethő.
A secure electronic exam system.


R. Haenni and O. Spycher.
Secure internet voting on limited devices with anonymized dsa public keys.

In *WOTE’11. USENIX, 2011.*