What Security for Electronic Exams?
(Extended Abstract)

Rosario Giustolisi, Gabriele Lenzini
SnT/University of Luxembourg, Luxembourg

Giampaolo Bella,
University of Catania, Italy

***Abstract*—Electronic exam systems are pieces of software employed in online educations to assess performances of students. However, both the security of the protocols they reply upon and a general understanding of the possible threats is still to be met. This manuscript outlines a Ph.D. research work wherein we attempt to shed some light in the area. We identify the phases composing a typical exam system, we comments on relevant security properties that should be preserved in the various phases, and we advance an informal though structured definitions of them.**

I. Introduction

Electronic exam (e-exam) systems are the new frontier in computer-based assessment and remote education. They are complex systems involving a number of parties such as examination authorities, candidates, invigilators, examiners. They rely on information and communication technology (ICT) at different degrees. For example, they can combine traditional pencil-and-paper assessment procedures with some level of automatic digital data processing (e.g., exam sheets can be scanned and transmitted to examiners for marking), or they can be fully computerized. In this case students take exams by interacting with a electronic device in either invigilated or non-invigilated environments.

E-exams are believed to promote quality and equity in education because they are supposed to offer objective evaluations of written exams and equal access to anyone. Example of e-exam systems are those used by the Educational Testing Service (ETS - http:\\www.ets.org) to run the IELTS [**?**], the GRE [**?**] and the TOEFL [**?**]. These tests evaluate every year the ability to use and understand English of millions of people from hundreds of different countries. Formerly deployed as traditional paper-based supervised tests, they have been re-engineered to be computer-based. The European Computer Driving License Foundation (ECDL - http:\\www.ecdl.com) employs supervised e-exam systems to assess basic skills and competencies for a proficient use of computers and common computer applications. Also the European Union adopts computer-based e-exam in the selection procedure for permanent and non permanent job positions for all the EU institutions (http:\\europa.eu/epso/apply/how_apply/index_en.htm).

A. The massive growth

In the last years e-exam systems have gained importance as a result of increasing interest in "Massive Open Online Courses" (MOOCs), the on-line platforms for a large-scale interactive participation and open access to courses and lectures via the web. MOOCs take advantage of various web-based technologies including video presentation and social networks to give students access to course contents. Platforms such as 'edX' (https://www.edX.org), 'Coursera' (https://www.coursera.org), and 'Udacity' (https://www.udacity.com) count already hundred of partners among which top-tier institutions such as Harvard, Stanford and MIT. Relevantly, MOOCs support e-exams as they offer internet-based assessment and remote marking for formative and summative tests.

B. Education in security

Whether e-exams, either in MOOCs or in other educational frameworks, will be capable to sustain and forward quality in education is a question that goes beyond the scope of our research. Beyond our interest is also to question how fair is to leave machines mark written tests. This issue, debated in [**?**], is contrasted by many institutions that prefer to have human to evaluate tests. But, whatever the framework and the way of marking tests, e-exams will fail their mission unless designed to be robust to frauds.

The risk of forgery is high, since almost all roles have an interest in behaving selfishly. Students may aim to get the highest marks with the least effort, a goal they can get by copying and other cheating. Also authorities may have motivation to tamper with the assessment results. For instance, in the scandal known as Atlanta Cheating[1] about 35 people among school administrators, educators, and superintendents manipulated ranks and scores with the goal of gaining more school governmental funds. Collusions among parties are also possible: authorities can try to interfere with the exam process for reason of favouritisms, nepotisms, or partisanship in favour of some candidates or candidate's supporters.

Such frauds are well known. To reduce the likelihood of cheating, in fact, traditional exams adopt procedures that have been built after years of experiences. On the contrary e-exam systems, regardless if the are invigilated and taken in reliable testing centres, are unprotected because of their using ICT. The shifting from traditional assessment procedures to the computer-based ones is critical. Unless different defences are in place to preserve the security properties provided by previous pencil-and-paper solutions, it will make the assessment process vulnerable to attacks and to frauds.

Indeed, even a general understanding of the security properties for pencil-and-paper exam systems is not documented anywhere. There is no list of security requirements, whereas the use of communication technologies, such as the Internet, will further expose e-exam systems to new threats which are impossible in the traditional setting.

[1] See "Atlanta Cheating Scandal", CNN.com, April 2013

The security properties that e-exam system protocols and processes aim to withstand, as well as the threats that they should thwart, should still meet a general understanding and clear specifications.

C. Checking our homework

Our goal is to set a framework for the study of security of e-exams. Ideally, security should not depend on trusted hardware, trusted parties, or trusted authorities; systems should be resilient to malicious threats even if they come from supposed honest elements or principals. Implementations should be, at least in some form, verifiable/auditable, accountable, or both.

Verifiability has been explored in application domains close to e-exams, namely e-voting and e-auction. In e-voting, *universal verifiability* (e.g., see [**?**]) states that a voter (resp., anyone) can verify the correctness of the voting results by using only public data. In e-auction, verifiability has been defined in [**?**] as the quality of allowing anyone (i.e., the winner, the seller, and the losers) to test the auction process and its output for integrity (e.g., only legitimate bids have been processed, the winning bid is the highest price, the loosing bids cannot win) provided that participants followed the auction protocol correctly.

Auditability is often considered as synonym for verifiability, although in certain contexts it may be seen as a weaker property. If the system has been designed in such a way to have data log, which may not be public, an auditable system allows an auditor to check for frauds once they have occurred (e.g., see [**?**]). Accountability [**?**] ensures that also the perpetrator can be identified.

II. Research Objectives

Our research attempts to define a research roadmap in the area of secure, verifiable, and accountable e-exam systems. We have identified three specific research objectives, each driven by concrete research questions.

Objective 1 - formalization of properties: The first objective is to clarify what are the security properties that are relevant for an e-exam system. In so doing, we have to define a model for an exam system, that is, to identify the typical phases that compose it and the roles therein involved. This paper already advances the description of such phases. Moreover, it proposes informal though structured definitions of related security properties (see Sect. III). A formal specification of such properties in a process algebra of choice is then within reach, although it is difficult to anticipate whether standard analysis tools can be efficiently used to check them automatically.

Comparing the security properties of e-exams with the ones of e-voting is an interesting part of this research objective. Properties such as vote anonymity and privacy, vote integrity and verifiability have surely some relevance in e-exams too, but in the context of e-exams they become more complicated and thus interesting to be fully understood, characterized, and studied. For example, while a vote must never be associated to its voter, an exam form should ideally be marked anonymously but eventually associated to its author.

Objective 2 - verification of security properties: The second objective is to verify whether existing e-exam protocols yield the security properties we have identified in objective 1. Also here we take inspiration from works in the related domains of e-voting and e-auction, whose results and research on security issues have been increased significantly in the last years (e.g., see [**?**], [**?**], [**?**]). Works on e-auction are yet preliminary (e.g., see [**?**]), but still inspiring. As threat analysis, we plan to adopt the approach already experimented in the Prêt à Voter verifiable voting system [**?**]. We intend to follow a formal method approach, possibly using the 'applied-pi calculus' and its model checker ProVerif [**?**], tools that have been proved of great flexibility in modelling voting and auction systems together with their relative security properties (e.g., see [**?**], [**?**], [**?**], [**?**]). We deliberately choose to analyse protocols that belong to different categories of e-exams. In particular, we refer to WATA [**?**], which is a computer-assisted exam protocol, and an internet-based protocol due to Huszti *et al.* [**?**].

Objective 3 - security design: The third research objective is more ambitious and likely to be left only when the other two will be achieved. It is about to design at least one new e-exam scheme that ensures relevant security properties that are missing by the systems analysed within the objective 2. The design of new protocols that meet our security requirements in each phase of the competition is challenging due to non-trivial problems, such as combining contradictory security requirements (anonymity vs. authentication) or having lightweight reliance upon trusted parties. These issues can be tackled by applying security mechanisms such as decryption mixes [**?**], conditional privacy [**?**], ElGamal encryption, and visual cryptography mechanisms [**?**], some of which have been already applied in e-voting. Again we aim at looking at this domain to find the right tools and methodologies of design. Part of this goal is to propose a design that mitigates strong trust requirements, for example by substitute fully trusted parties with lightweight trusted third party as done in [**?**].

III. What is in progress

A. E-exams: Players and Phases

We have identified the players and the phases that compose a general e-exam process.

Players: An e-exam has at least two kinds of participants: the *candidates*, who intend to sit for the exam, and the *examiner*, who marks the answer submitted by candidates. This model can capture face-to-face examination such as periodical academic assessment, in which the examiner also manages the exam procedures. In other situations, such as qualifying examination or internet-based exam, it seems to be more appropriate to assign the role of managing the exam procedures to an *examination authority*, limiting the duties of examiners to the evaluation of answers. The examination authority can be further split into different roles according to specific exams: *invigilators* ensure that no candidate cheats, while *question committees* generate exam questions.

The participants outlined above may potentially act malevolently and even collude. Interestingly, this poses different threat models that depend on the malicious participants.

Phases: A typical e-exam can be conveniently split up into four different phases: *registration*, *examination*, *marking*, and *notification*. At *registration*, the examination authority creates a new examination and checks eligibility of the candidates who attempt to register for it. Only candidates who pass the standard eligibility criteria, such as payment of fees and previous qualifications, get successfully registered. At *examination*, each registered candidate gets an exam form with questions, answers the questions, and submits her answer to the examination authority. The exam form may also include the candidate's identification details. The examination phase should be supervised in order to ensure that no candidate cheats. At *marking*, the exam form is eventually given to the examiner, who marks the answer. The exam form should not reveal the real identity of the candidate to ensure anonymous marking. The exam terminates with the *notification*, in which marks are assigned to their respective candidates. Assigning a mark means that each candidate is delivered her mark. Depending on a specific exam, the delivery can be remotely or *de visu*. The latter is the case when the answers are evaluated immediately after the examination by means of electronic marker.

B. Categories of E-exams and Security Properties

We have identified the categories of e-exams and listed relevant security properties common to those categories.

Categories: E-exams differ from traditional pencil-and-paper exams because they employ partially or completely ICT. An e-exam can be *computer-assisted*, when ICT is used in any phase of the exam. For example, when the examination is accomplished by paper-based forms, while registration and notification are carried out remotely. An e-exam is *computer-based* when the exam is taken on computers, or finally it can be *internet-based* when the exam activity requires the use of the internet.

Security Properties: Despite the evident differences among the three categories, the distinction in players, the various items, and even the security properties that are spelled out below can be instantiated on each of them. For example, the 'exam form' is, for paper-based exams, the piece of paper where the candidate enters her answer, while it is a file for computer-based or internet-based exams. In the latter case, the invigilators can be validation pieces of software filming a candidate while she is filling up the form with her answers, and also sealing the association between the video and the filled form.

Having clarified the players, the phases, and the categories that characterize e-exam systems, we introduce and comment a set of security properties. The set is not meant to be comprehensive but includes what we think are the most relevant properties for each phase.

Registration Phase:

Property 1 (Candidate Eligibility): Only candidates who pass the official eligibility criteria for an exam get the credentials to register for that exam.

This properties ensures that only who is eligible for an exam will be able to participate to it and thus to appear in the registration list for that exam.

Examination Phase:

Property 2 (Candidate Identification): The identity of a registered candidate is correctly verified.

Candidate identification can be established by checking the candidate's valid ID token (e.g., a student card) in face-to-face exams. Credentials given at registration can also be checked for authenticating the candidate in remote exams.

Property 3 (Candidate Authorization): Only a candidate who has registered for an exam can participate to that exam.

Candidate authorization follows from verifying that the authenticated candidate is also in the list of registered candidates produced during the registration phase and made available at examination phase.

Property 4 (Form Authentication): An exam form is correctly associated to the authorized candidate who is taking that exam.

Personal details of the authorized candidate can lay on the candidate's exam form. For traditional exams, the examiner can check that the candidate writes down the right personal details on the form, or she can write them down personally. However, we stress that the exam form is intended to contain the answer, thus it does not necessarily include the candidate's detail and other strategies are possible. For computer exams, the examiner could equally check what details the candidate enters. For remote exams, remote validation software is necessary.

Property 5 (Answer Authorship): The answer of a candidate gets correctly associated with the candidate's authenticated form.

This property says that a candidate's answer can never be associated with another form but hers, as it happens when two candidates swap their forms. It can be satisfied by establishing form authentication and enforced by the invigilators.

Marking Phase:

Property 6 (Form Integrity): No one can alter the forms after they have been submitted by the candidates.

An answer cannot be modified after the candidate submits it in her exam form. Likewise, it ensures that her form cannot be illicitly assigned to anyone else.

Property 7 (Anonymous Marking): The examiner cannot associate an answer to any candidate.

This version of anonymous marking signifies that the examiner marks a form while ignoring its author — it can contribute to the fairness of the marking.

Property 8 (Strong Anonymous Marking): No one but the candidates can associate an answer to any candidate.

The strong version of anonymous marking says that also the examination authority is unaware of the author of an answer while the answer is being marked. An implication is that a candidate anonymity during the marking will even resist collusion of examiner and examination authority.

Notification Phase:

Property 9 (Mark Integrity): The mark that the examiner gives to the form on behalf of a candidate is assigned to that candidate only.

Once the examiner produces an official mark for a candidate, the mark cannot be changed, and will be officially linked to that candidate.

Property 10 (Mark Privacy): The association between an answer and its corresponding mark is not known to any candidate than the author of the answer.

This property ensures that the mark assigned to a candidate is known only to her and possibly to the examination authority, which assigns the mark.

IV. Related Work

The research community has shown interest in e-exam security only recently. Invigilation software such as [**?**], is the result of the increasing popularity of MOOCs. However, invigilation tackles only one of the possible threats in e-exam, that is, candidate cheating. Malicious examiners and exam authorities should be also considered as realistic threats in e-exam environment.

To our knowledge, there is no work that has a formal approach in analysing the security properties for e-exam. Unlike similar systems (i.e, e-voting and e-auction), works on e-exams focuses only on the design, omitting a rigorous security analysis of the proposed scheme.

Currently, the most comprehensive work is due to Huszti et al. [**?**]. They propose an internet-based protocol that aims to achieve a number of security properties, without the existence of a Trusted Third Party. The authors claim to accomplish the security requirements by applying three main cryptographic building blocks: ElGamal encryption, reusable anonymous return channel, and timed-release service. However, the paper provides only an informal analysis of the security property.

Bella et al. propose WATA [**?**], a computer-assisted system that uses conventional printouts and gives the ability to de-anonymise an exam solely to its author. The system can be managed remotely and is employed to evaluate master students. The protocol and its security analysis are presented rather informally.

NEMO-SCAN [**?**] uses a patented anonymity paper cover: one part hides the candidate details, while another contains a section in which examiners write the marks down. At notification time, a scanner with a proprietary software scans the paper with the candidate details, and assigns it the mark. The system is primarily meant to achieve anonymous marking, while it is not clear if it possesses other related security properties.

Other works focus on countermeasures to avoid cheating during online exams [**?**], [**?**], [**?**], and advance methods to ensure the authentication of the candidates [**?**], [**?**]. However, such methods assume full trusted examination authorities, and preclude anonymous marking.

Several papers study the security properties of e-learning systems [**?**], [**?**]. In particular, relevant works analyse authentication and privacy issues of teachers and students, and propose some ideas on how ensure security in such systems [**?**]. However, major risks of e-learning appear to be significantly different from ones of e-exams. While the former are more susceptible to external threats, e-exams have to tackle more with insider threats, such as cheating candidate or corrupt examiners.

V. Conclusions and Ongoing Work

Despite the widespread use and importance of e-exam systems implementing various dedicated protocols, research in this area only seems to be at its dawn. Certain institutions still rely on an 'anonymising office' that gives each candidate a pseudonym. The candidate has to write the pseudonym down in the exam form at examination phase, with the purpose of hiding the candidate's identity during the marking. However, candidates have to trust the anonymising office not to collude with the examiner.

This abstract conjectured that removing such trust by means of an anonymous marking property is perhaps the main *raison d'être* of a modern e-exam protocol. This and other properties are oriented at protecting the candidate from both examiner and examination authority, and hence appear to come into play at marking and notification phase. By contrast, properties of the registration and examination phases aim to protect the authorities from cheating candidates.

Our ongoing work is to analyse existing e-exam protocols (e.g., [**?**], [**?**]). Informal reasoning and initial attempts at formalisation have already shown a number of weaknesses. These appear to justify the design of a new hierarchy of e-exam protocols that compel participants to only see a share of sensitive information such as the candidate personal information during marking.

This research has just started, but has already clarified that e-exams properties differ from and seem to complicate their nearest relatives, which are e-voting and e-auctions. For example, a high-level property of e-exams is that answer authorship should be preserved even in the presence of colluding candidates. Conversely, vote authorship is not a problem for e-voting, in fact unlinkability between voter and vote is a desired property. Strong anonymous marking, which is meant to hold during the marking but will be trivially falsified after notification, evaluates to a sort of fixed-term anonymity, which is eventually going to be resolved. This is more in line with the properties of a sealed e-auction winning bid than with those of an e-voting ballot. However, the threat models for e-exams and e-auctions seem different: while collusion between candidates results appropriate for e-exams, competitiveness among bidders motivates e-auctions. Validating these observations is our goal for the near future.