Master Thesis Proposal

Analyzing Accountability in (E-)Exams

Supervisor: Jannik Dreier and Ralf Sasse
Professor: Prof. D. Basin
Issue Date: 2015
Submission Date: TBD

1 Introduction

Many companies and universities increasingly use electronic exam (e-exam for short) systems: for example Cisco’s CCNA certifications or language tests such as IELTS or TOEFL are organized using computer systems, and also at ETH Zurich electronic exams are held regularly [8]. This naturally raises the question of the security of such systems. From the point of view of the organizing institution, cheating is a major concern, but candidates (i.e., students) are typically more concerned with fairness and transparency of the process. In particular the latter concerns are often ignored by current systems. Typically the system is assumed to be trusted, and the candidates can only partly verify whether everything went well. Yet, as recent scandals have shown [2, 5], (e-)exam systems cannot always be trusted entirely.

In security protocol design the notions of Verifiability [1, 7, 3], Accountability [7] and Auditability [6] have been known for some time. A verifiable protocol protocol allows the participants to verify, after the protocol’s execution, whether the outcome of the protocol is correct. When verifiability fails, accountability additionally allows to identify which party is responsible for this failure. Finally a protocol is auditable if it logs sufficient evidence to convince an outside judge of the absence of errors.

Some preliminary work on verifiability in e-exams exist [4], however accountability and auditability have not yet been studied in this context.

2 Assignment

2.1 Objectives

The goal of this project is study accountability and auditability of (e-)exams. In the first part, based on previous work, formal definitions of accountability and auditability have to be developed. This requires identification of the stakeholders, and the properties requiring verification. Moreover, a suitable model for the definitions has to be chosen.

In the second part, these definitions will be applied on a case study. The goal is to validate the model and the definitions, but also to analyze to which extent current systems ensure the desired properties. Possible case studies include existing real e-exam systems (e.g., the system used at ETH), or cryptographic protocols from the literature. A formal analysis using a protocol verification tool such as Tamarin, ProVerif, CryptoVerif or similar is expected.

Optionally also a traditional pen-and-paper exam system can be studied, or new and improved e-exam protocols can be proposed. Moreover, if shortcomings in the case studies are identified, fixes can be developed.
2.2 Tasks
- Identify and analyze relevant related work
- Propose a model and definitions of accountability and auditability in e-exams
- Choose a case study, and obtain its description
- Formalize the case study in the developed model, and analyze it using a protocol verification tool
- Evaluate the results
- Optional: Fix identified shortcomings in the case studies, and validate the fixes
- Optional: Propose a new and entirely accountable and auditable e-exam protocol

2.3 Deliverables
- At the beginning of the semester thesis an agreement must be signed which allows the supervisor of this thesis, his project partners and ETH Zurich to use and distribute the software written during the thesis.
- At the end of the second week, a detailed time schedule of the semester thesis must be given and discussed with the supervisor.
- At the end of the semester thesis a presentation of 30 minutes must be given during an Infsec group seminar. It should give an overview as well as the most important details of the work.
- The final report may be written in English or German. It must contain an abstract written in both English and German, this assignment and the schedule. It should include an introduction, an analysis of related work, and a complete documentation of all used software tools. Three copies of the final report must be delivered to the supervisor.
- Software and configuration scripts developed during the thesis must be delivered to the supervisor on a CD-ROM.

References
