Formal Analysis of Electronic Exams

Jannik Dreier[1], Rosario Giustolisi[2], Ali Kassem[3]
Pascal Lafourcade[4], Gabriele Lenzini[2] and Peter Y. A. Ryan[2]

[1] Institute of Information Security, ETH Zurich, Switzerland
[2] SnT/University of Luxembourg, Luxembourg
[3] Université Grenoble Alpes, CNRS, VERIMAG, Grenoble, France
[4] Université d'Auvergne, LIMOS, France

1 Abstract

Universities and other educational organizations are adopting computer- and internet-based assessment tools (herein called electronic exams, or *e-exams* for short) to reach widespread audiences. While this makes examination tests more accessible, it exposes them to new threats. Most current work on e-exam systems aims at mitigating the risk of cheating, but recent scandals have shown that such systems are also vulnerable to other attacks. In particular it turned out that not all exam authorities can always be trusted, and that the use of networks makes the systems vulnerable to outside attackers. Although not employed in practice, in the scientific literature there are some proposals of protocols trying to address these risks.

However, there are very few strategies to check such e-exam protocols for security, and there is a lack of precise formal security definitions in this domain. This paper fills this gap: in the formal framework of the applied π-calculus, we define several fundamental authentication and privacy properties and establish the first theoretical framework for the security analysis of e-exam protocols. In particular, we consider authentication and integrity of the questions and answers, as well as privacy of marks and secrecy of the questions before the exam. Moreover, we also analyze anonymity of the examiners and candidates during the grading process to ensure fairness.

As proof of concept we analyze two e-exam protocols with ProVerif, an automated protocol verification tool. The first "secure electronic exam system" proposed in the literature turns out to have several severe problems, and fails at ensuring all analyzed properties. The second protocol, called *Remark!*, is proved to satisfy all the security properties assuming access control on the bulletin board. We propose a simple protocol modification that removes the need of such assumption though guaranteeing all the security properties.

Keywords: Electronic Exams, Formal Verification, Authentication, Privacy, Applied π-Calculus, ProVerif