ABSTRACT

Security is one of the main problems in Web-based assessment systems, particularly in guaranteeing the non-repudiation of test submissions. The authors have developed EVAWEB, a Web-based assessment system that addresses this issue by using digital signatures. Moreover, the use of this technology in EVAWEB provides a real context to students for learning how digital signatures work. This article focuses on the enhancements that have been incorporated into EVAWEB in order to develop an improved second version of the system.

Keywords: digital signatures; innovation; non-repudiation; security; teaching; Web-based assessment; X.509/PKIX framework

INTRODUCTION

Security and privacy issues stand as some of the main problems of existing e-learning systems (Chan, Leung, & Li, 2003; Warren & Hutchinson, 2003). Particularly, online assessment has been largely debated because of difficulties with properly authenticating students and making their submissions nonrepudiable. Non-repudiation is defined by the International Organization for Standardization (ISO) as the security property that provides protection against false denial of having been involved in a communication (ISO/IEC 7498-2, 1988).

Non-repudiation of submitting and receiving a test is a desirable property in online assessment. This property is usually provided by logs in most known e-learning systems such as WebCT or Blackboard. Although digital signatures provide non-repudiation security services (ISO/IEC 13888-3, 1997; Zhou, 2001), these systems do not include this technology yet.

On the other hand, the understanding of digital signatures is crucial for students in information technologies and, to some extent, also for the general public as electronic signatures have been given legal recognition recently in several
countries. Traditionally, computer security curricula of undergraduate computer engineering programs include laboratory sessions that allow students to learn digital signature technology in practice using tools such as PGP and OpenSSL. As in many study areas, the student learning process can be enhanced if learning by doing in context is used instead of making the students solve a set of naïve academic exercises (Hsu & Backhouse, 2002).

The authors have developed EVAWEB (González-Tablas, Wouters, & Ramos, 2004; González-Tablas, Wouters, Ramos, & Ribagorda, 2007), a Web-based assessment system that focuses on non-repudiation requirements through the use of digital signatures. Furthermore, EVAWEB enhances the students’ learning of digital signatures by providing them a real context to practice this technology. It has been developed in the context of an innovative education experience for the teaching of security in information technologies at higher education levels. The students learn the concepts involved in digital signatures, using them in their own assessment process. It is important to note that EVAWEB does not intend to be used in real distant education but in proctored environments. The higher security required for nonproctored exams would need stronger authentication solutions.

The evaluation of EVAWEB by some students of Universidad Carlos III de Madrid has turned out as an above-average success, but, at the same time, results highlighted the need for improvements in the system (González-Tablas et al., 2007). In this article, the enhancements that have been incorporated into EVAWEB in order to obtain a second version of the system are presented. The improvements are mainly focused on architecture, functionality, portability, interface, database, and security aspects.

The remainder of the article is organized as follows. First, previous work is reviewed. Second, the functionalities and architecture of EVAWEB Version 1 (v1) are described. Then, the enhancements that have been incorporated into EVAWEB are shown. Finally, the conclusions and future work are exposed.

PREVIOUS WORK

PGP/GnuPG (PGP) can be used to digitally sign essay-type tests and send them by e-mail, but PGP is more used for informal authentication because of the Web-of-trust paradigm it uses. The authors do not know about an e-learning tool that integrates X.509/PKIX-based digital signatures in Web-based online assessment. This might seem odd as these signatures are largely used in other areas such as e-government, e-commerce, or even higher education administrations for providing authentication and non-repudiation, and there exist proprietary software that enables electronic form signing. In addition, currently several researchers propose the deployment of PKI as a solution for most of the security problems in higher education (Dartmouth College PKI Lab, 2001; Steinmann, Zimmerli, Jampen, & Braun, 2002; Sura & Mukkamala, 2003). The Dartmouth PKI Lab points out explicitly the use of this technology to provide non-repudiation in assessment. Although there are advantages offered by this framework, derived from having a centralized source of trust, the deployment and maintenance are harder than those faced by other trust models. This could be one of the reasons some discourage its full integration in e-learning environments, or at least in e-learning tools. The authors think that once higher education deploys PKIs for its institutions, the main e-learning tools will integrate this technology also.

There exist other proposals that use cryptography in order to get confidentiality for the answers (Lee et al., 1997) or integrity and authentication by means of hash functions (Shafarenko & Barsky, 2000). Most proposals use mainly strategies such as securing browsers, monitoring students, mandatory initial log-in of a proctor, logs, access control from some range of IP (Internet protocol) addresses, assessment available during certain limited time periods, shuffle choices and randomized questions to avoid students cheating beside authentication (Lister & Jerram, 2001; Pain & Le Heron, 2003; Shepherd, 2003). Nevertheless, they lack the non-repudiation service that digital signatures provide.
Are Accessible Distance Learning Systems Useful for All students?: Our Experience with IMES, an Accessible Web-based Learning System
Ana Iglesias, Lourdes Moreno, Elena Castro and Dolores Cuadra (2014). International Journal of Web-Based Learning and Teaching Technologies (pp. 1-17).
www.igi-global.com/article/are-accessible-distance-learning-systems-useful-for-all-students/109541?camid=4v1a

The Pivotal Role of Faculty in Online Student Engagement and Retention
www.igi-global.com/chapter/the-pivotal-role-of-faculty-in-online-student-engagement-and-retention/140641?camid=4v1a