IGI PUBLISHING **ITJ4123**

701 E. Chocolate Avenue, Suite 200, Hershey PA 17033-1240, USA
Tel: 717/533-8845; Fax 717/533-8661; URL-http://www.igi-global.com

This paper appears in the publication, **International Journal of Web-Based Learning and Teaching Technologies**, Volume 3, Issue 1
edited by **Liliane Esnault**

EVAWEB V2:
Enhancing a Web-Based Assessment System Focused on Non-repudiation Use and Teaching

A. I. González-Tablas, Universidad Carlos III De Madrid, Spain

A. Orfila, B. Ramos, Universidad Carlos III De Madrid, Spain

A. Ribagorda, Universidad Carlos III De Madrid, Spain

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; Steinemann, 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.

EVAWEB V1: DESCRIPTION AND EVALUATION

EVAWEB v1 allows teachers to administrate the creation and modification of tests for different subjects and groups of students as well as to assess the students automatically. The most innovative feature of EVAWEB is that neither can students repudiate the fact of having done a test (and the concrete answers) nor can teachers deny the reception of the test and the automatically generated mark. This is achieved using X.509/PKIX-based digital signatures.

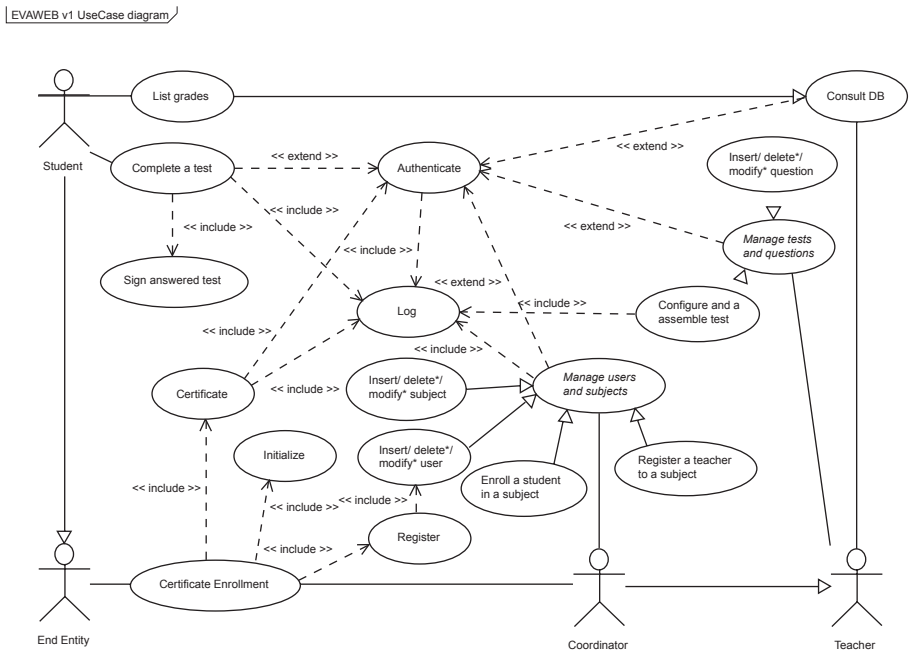
Students must enroll into the PKI before they can use any of the enabled services. In EVAWEB, this step occurs at the same time as the registration to the Web-based assessment system. The system issues a password to the student that he or she must use for subsequent authentication. The first time the student logs into the system, he or she must submit a photograph and request a certificate. Thus, the student uses a key generation tool to generate a key pair and the associated certificate request. He or she stores the private key in a file, encrypted with a passphrase, and submits the certificate request to the server. Then, he or she has to meet the teacher in charge of the subject to finish the enrollment process. The teacher verifies the identity of the student (analyzing if personal data in the certificate request really corresponds to the student and if his or her photograph matches and is recent) and asks EVAWEB to sign the corresponding certificate. Finally, the student can download this certificate from the Web site. Once this operation is fulfilled, the student can request a certificate revocation before its expiration date in order to make it invalid.

To submit an answered test, students sign the hash of their answers and some other personal data. In EVAWEB, the signature is performed outside the Web browser by an applet signed by the server. To generate the signature, first, the signed applet shows the student the answered test. Second, the student indicates where the private key is stored and types the password that decrypts it. Then, the signing applet generates the signature (using the student's private key), appends it to the answered test, and submits all to the server. Once the server receives the signed test, the signature is verified. EVAWEB will not accept a submission if the signature is incorrect. If the verification has been successful, the server calculates the grade and returns the student a signed receipt of his or her assessment submission, including the grade. The student can verify the server's signature and save the receipt. Therefore, non-repudiation of origin and receipt is fulfilled.

Users and Functionalities

A use-case diagram of the functionality of EVAWEB v1 is shown in Figure 1. EVAWEB v1 distinguishes between two main types of users: teachers and students. Some teachers have extra privileges because they are coordinators of subjects. Thus, coordinators perform the task of system administrators: They manage users (students, teachers) and subjects. As they have responsibility on the subjects they coordinate, they are in charge of registering any additional teachers to the corresponding subjects and enrolling students to their respective subjects. Teachers and coordinators registered to a subject can manage the subject's tests and question pool, and can also consult the system's database. Any teacher associated with a subject can add questions to its question pool, and modify and delete them if they are not used in any test. Teachers also control the time a test is available online for authorized students. Then a student has access to a test only after a process of authentication and to those tests teachers want. When a student finishes answering, he or she must submit the answered test to the system. Before submitting it, the student must sign it. Once the test has been answered, signed, and submitted, it is stored and assessed in the server, and the student receives a signed confirmation of his or her submission and the obtained grade. Therefore, students operations are just related to performing tests and consulting grades. Obviously, both teachers and students can consult previous test grades but, in the case of students, only their own grades.

Figure 1. Use-case diagram showing functionality of EVAWEB v1 (González-Tablas et al., 2004)



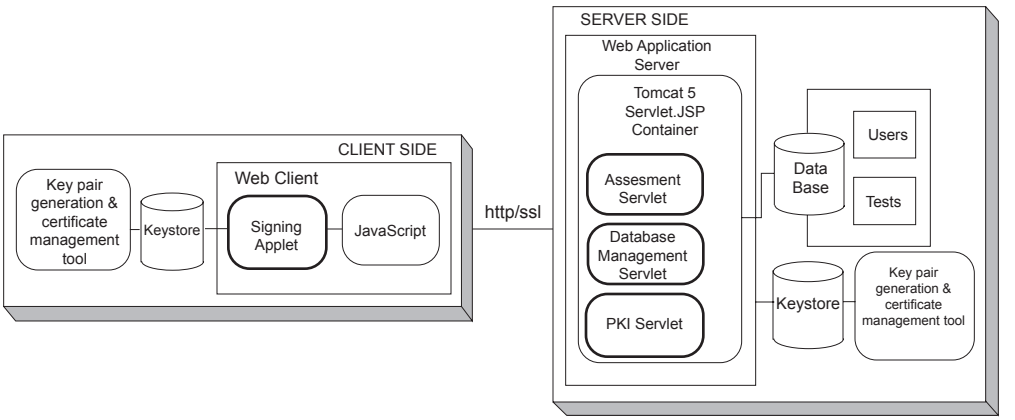
Architecture

EVAWEB v1 has a three-tier architecture (see Figure 2) composed by a Web application running on a servlet container on the server side, and a Web client supported by some processing capabilities on the client side. On the server side, three main modules can be identified that have been implemented with three servlets: the assessment servlet, the database management servlet, and the PKI servlet. The assessment servlet is in charge of serving students' test requests and processing the test answers. The database management servlet is used for consulting, inserting, modifying, and deleting users, subjects, and tests in the database. The PKI servlet is in charge of providing the basic functionality of a PKI. In addition, there is also a database with users and test information, and a repository that contains both the certificate authority (CA) keys and the student public-key certificates (needed to verify the signatures). On the client side, JavaScript is used to perform local form validations and to improve interactivity. The signature on the client side is performed via a signing applet, which communicates with the user through Java graphical interfaces and with the browser via JavaScript. Further details on the implementation of EVAWEB v1 can be consulted in González-Tablas et al. (2004).

Signature Process

Signing is performed outside the Web browser, similar to a smart-card signature in which the signature is generated inside the card and the private key never leaves the card. The process is as follows. First, a signed applet shows the student his or her answered test. The use of a signed applet allows the recipient to verify the authentication and integrity of the code. Furthermore, it provides a way for identifying which code is authorized to execute with special permissions not given by default inside the Java

Figure 2. Architecture of EVAWEB v1 (González-Tablas et al., 2004; González-Tablas et al., 2007)



sandbox (such as reading local files). Second, after revising his or her answers, the student indicates where the private key is stored (e.g., student's pen drive) and types the password that protects the key. Finally, the signing applet performs the signature, appends it to the answered test, and submits it to the server.

Other Security Features

Users authenticate with a user name and password mechanism, and the student's photo can be seen on the test page while the test is being answered. This biometric measure reduces the risk of a physical impersonation attack. To provide confidentiality, every communication with the Web application server relies on the SSL protocol. Role-based authorization (teacher, coordinator, and student) is enforced in order to access Web application components. Furthermore, the IP's range and time-window access control is enforced when students perform tests. Non-repudiation of students' submissions is achieved by X.509/PKI-based signatures. Finally, the use of cookies and servlet context variables contribute to preserve session security.

Evaluation of EVAWEB v1

EVAWEB v1 has been assessed by the students of Universidad Carlos III de Madrid in the context of an innovative education experience (González-Tablas et al., 2004; González-Tablas et al., 2007). The experience turned out an above-average success, but results and a further analysis highlighted the need for improvements in the system, which are described next.

Functionality

EVAWEB v1 has a restricted set of functionalities related to the management of the database. Particularly, it is not possible to modify or delete data. In addition, EVAWEB v1 requires the realization of annoying manual processes for issuing each student certificate as the PKI servlet only allows one to upload certificate requests and download issued certificates. This limited functionality reduces usability from the point of view of teachers and increases the probability of errors during the certificate issuance process.

Interface

Form data validation is not complete in EVAWEB v1, so there is a high risk of system breakdown because of unexpected errors during the processing of input data. Furthermore, the communication with the user is done through HTML (hypertext markup language) pages, which are generated one by one in the servlets. This deficiency reduces system maintenance

because if a modification in the interface is needed, each piece of code that generates HTML pages has to be changed, which, besides being a tedious process, has a very high probability of error.

Database

EVAWEB v1 presents some minor deficiencies in the design of the database that make the scalability of the system difficult.

Architecture

EVAWEB v1 does not follow any concrete architectural design pattern; furthermore, presentation is mixed with the system's logic and access to the database is spread throughout all code. This kind of design is maybe valid for an initial demonstrator, but the maintenance and portability of the system is highly hindered.

Security

A security vulnerability in EVAWEB v1 is that users' passwords are stored clearly within the database. Furthermore, in the session initiation process, the user is not asked if he or she wants to access the system as a teacher or as a student. As the system first checks if there is any student with a specific identification, a teacher with such identification would not be able to access it (at least, as a teacher).

Logs

EVAWEB v1 presents annotations of actions done in the system through the Web application server console. This annotation mechanism is insufficient as the console may be closed leading to the loss of system actions. In addition, using the Web application server console as a log mechanism makes it difficult to have separate logs concerning different aspects of the application.

Portability

This characteristic is quite restricted in EVAWEB v1. First, the database is implemented with Microsoft Access, which restricts deployment to hosts using Microsoft Windows. Second, all the system's configuration information (directory paths, passwords, etc.) is defined within the code, meaning that if the system needs to be deployed in a different context, code must be changed and rebuilt.

EVAWEB V2 AS AN ENHANCEMENT OF EVAWEB V1

A second version of EVAWEB has been implemented to address the deficiencies of EVAWEB v1. System users remain the same: teachers and students. Changes introduced in the system are described as follows.

Functionality

Functionality of EVAWEB v2 has been first restructured (see Figure 3), incremented, and enhanced. Modification and deletion of data (users, subjects, tests, and questions) is now possible. Furthermore, EVAWEB v2 now allows teachers to issue students' digital certificates with a very simple and automated process accessible from the Web interface. Student enrollment has been enhanced. Now it is possible to enroll several students at the same time to a subject. In addition, data queries now can be done based upon filters such as the date for tests or the enrolled subject for students, and from the query results, further related data may be accessed.

Interface

Navigability through interface Web pages has been refined, mainly aspects related to form validation. Usability has also been enhanced by redesigning the aesthetics of Web pages at the same time that modularity and maintainability have been greatly improved with the use of Web style sheets (see Figure 4).

Database

The database in EVAWEB v2 has been redesigned following the entity-relationship model shown in Figure 5. In this case, a teacher can be associated with or collaborate in one or more subjects, while a subject must always have a teacher associated with it. In addition, a teacher

Figure 3. Use-case diagram showing functionality of EVAWEB v2

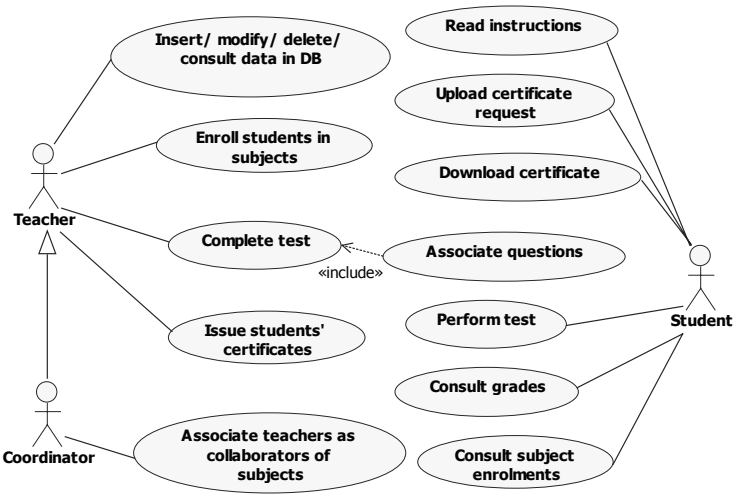


Figure 4. Use of Web style sheets in EVAWEB v2


```
body {
    background-image: url( "../imagenes/fondonormal.jpg" );
    font-family: Verdana, Arial, Helvetica, sans-serif;
    font-size: 12pt;
    color: black;
}

table {
    background-color: gainsboro;
    border: darkgray
}

.listado {
    background-color: lightsteelblue;
    font-family: Verdana, Arial, Helvetica, sans-serif;
    color: black;
    text-align: left;
}

.cabeceralistado {
    background-color: darkgray;
    text-align: center;
    font-family: Verdana, Arial, Helvetica, sans-serif;
    font-size: 14pt;
    color: white
}

.cabeceralistado2 {
    background-color: darkgray;
    text-align: left;
    font-family: Verdana, Arial, Helvetica, sans-serif;
    font-size: 14pt;
    color: white
}

h1 {
    font-size: 20pt;
    color: #000000;
    text-align: center
```

```
<%@ page contentType="text/html;charset=ISO-8859-1" language="java" %>
<jsp:include page="permisosProfesor.jsp"/>
<html>
<head>
    <title>
        Introducir datos
    </title>
    <META HTTP-EQUIV="Pragma" CONTENT="no-cache">
    <META HTTP-EQUIV="Expires" CONTENT="-1">
    <script type="text/javascript" language="JavaScript"
    src="js/comprobaciones.js"></script>
    <link rel="stylesheet" href="estilos/estilos.css">
</head>

<body>

<p align="right">
    <a href="menuProfesor.jsp" target="_self"><img
    src="imagenes/return.gif" border="0" alt="volver"></a>
</p>
```

can coordinate none or several subjects, but a subject always has a unique coordinator. A subject can have several tests, which are restricted to a single subject. A test can be composed of several questions and questions can be part of several tests, so questions can be reused. Questions, as well as tests, are restricted to a single subject and may have from one to four possible answers (with only one being true). Students may be enrolled to several subjects and subjects may have several students enrolled. A student can perform a test belonging to a certain subject whenever he or she is enrolled to that subject. Under this condition, a test may be performed by several students.

Architecture

The most important change in EVAWEB v2 affects its software architecture, which has been redesigned to use the model-view-controller design pattern in the server side to enhance its modularity and to ease its maintenance. The enhanced architecture can be seen in Figure 6. The client side remains the same as in EVAWEB v1. In EVAWEB v2 presentation, business logic and controller processes are separated by using JSP pages, servlets, and normal Java classes. Furthermore, access to the database is encapsulated through a Java class that acts as an interface.

Security

To solve EVAWEB v1 problems, users are forced to choose if they want to access the system as teachers or as students. Besides this, user passwords are not stored clearly anymore; instead, the database contains a hash of the password of each user. When a user attempts to log in, the hash of the password sent by the user is computed and compared with the one stored in the database in order to grant access.

Figure 5. Entity-relationship model used in EVAWEB v2

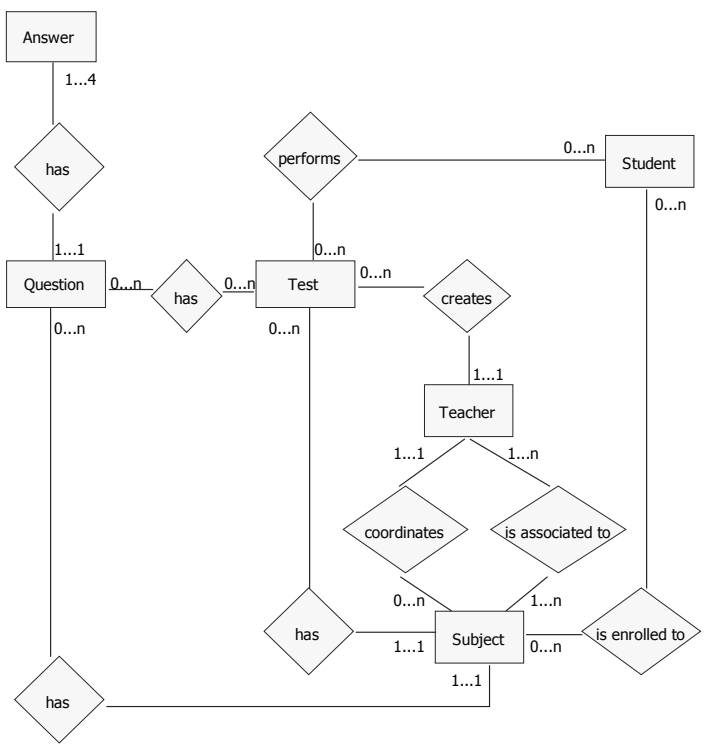
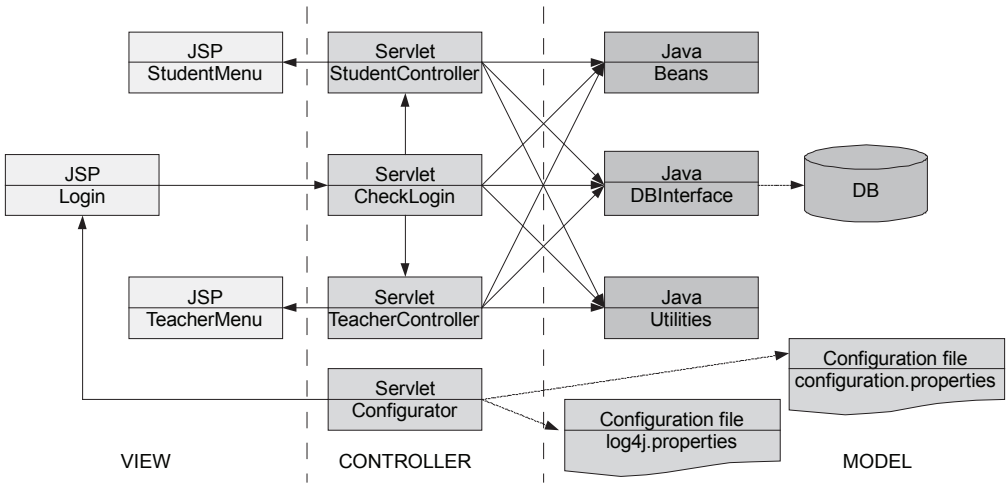


Figure 6. Architecture of EVAWEB v2



Logs

In EVAWEB v2, a log framework has been integrated that allows the registration of all actions taken in the system. Furthermore, the results of the tests submitted by the students are doubly logged in one file and then in a separate file to ease its query. In Figure 7, partial content of the main log is shown.

Portability

To enhance the portability of the system, first, the database management system has been migrated from Microsoft Access to MySQL. Second, configuration files have been created allowing the specification of installation variables, directory paths, passwords, and so forth. Examples of these configuration files are shown in Figure 8.

CONCLUSION

One of the main security problems in online assessment is making students' submissions nonrepudiable. The authors have developed EVAWEB, a Web-based assessment system that focuses on non-repudiation requirements through the use of digital signatures. Furthermore, the developed system aims to enhance students' learning of digital signatures by providing them with a real context to practice this technology. Thus, students learn the concepts involved in digital signatures, using them in their own assessment process.

A first version of EVAWEB was evaluated successfully by some students of Universidad Carlos III de Madrid. However, the evaluation highlighted also the need of some improve-

Figure 7. Main log file in EVAWEB v2

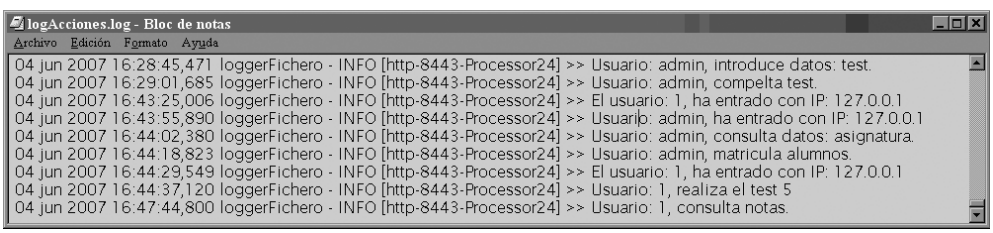
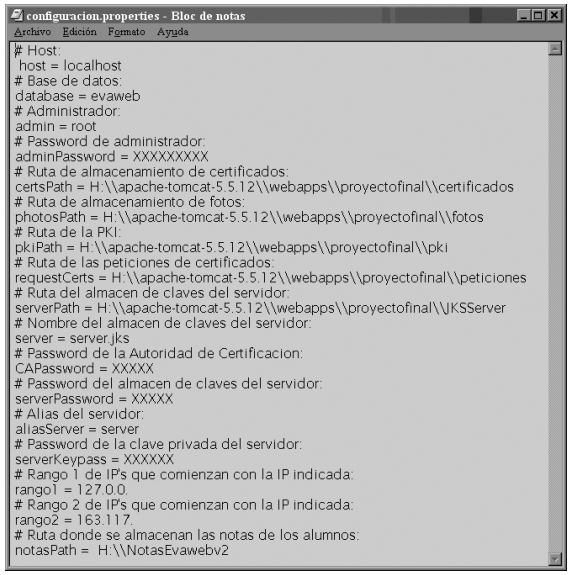


Figure 8. Configuration files in EVAWEB v2



ments in the system. These enhancements have been incorporated in a second version of the EVAWEB system and are mainly focused on architecture, functionality, interface, database, portability, and security aspects.

Main future work includes the evaluation of EVAWEB v2 by students in order to assess the effectiveness of the changes that have been introduced. In addition, new functionalities, such as the generation of statistics and printable documents (e.g., tests and reports) will be added. Up to now, only multiple-choice questions with one valid answer can be defined. EVAWEB should allow in the future multiple-choice questions and other features (such as fill in the blank, drag and drop, numeric entries, etc.). Security features can also be enhanced. For instance, smart cards could be used to sign the tests,

and digital certificates or biometric technology would improve student authentication process. Implementation of the model-view-controller design can be further enhanced if some Web application framework, such as Struts, is used. Finally, EVAWEB should be adapted to comply with Web accessibility guidelines (World Wide Web Consortium [W3C], 2006).

ACKNOWLEDGMENT

The authors acknowledge the work done by David Sánchez Torre and Javier Rodríguez Gandía in the implementation of, respectively, the first and second versions of EVAWEB while being students of Universidad Carlos III de Madrid. This work was partially supported by Universidad Carlos III de Madrid under 1ª Convocatoria de Apoyo a Experiencias de Innovación Docente Curso 2003-2004.

REFERENCES

Chan, Y.-Y., Leung C.-H., & Li, J. K. (2003). Evaluation on security and privacy of Web-based learning systems. In *Proceedings of the 3rd IEEE International Conference on Advanced Learning Technologies: ICALT'03*, Athens, Greece (pp. 308-309).

Dartmouth College PKI Lab. (2001). *PKI applications in academic computing.* Retrieved from http://www.cs.dartmouth.edu/~pkilab/acapps.shtml

González-Tablas, A. I., Wouters, K., & Ramos, B. (2004). Teaching X.509/PKIX based digital signatures while enhancing non-repudiation of a Web based assessment system. In *Proceedings of the IADIS International Conference WWW/Internet*, Madrid, Spain (Vol. 1, pp. 43-51).

González-Tablas, A. I., Wouters, K., Ramos, B., & Ribagorda, A. (2007). EVAWEB: A Web-based assessment system to learn X.509/PKIX digital signatures. *IEEE Transactions on Education, 50*(2), 112-117.

Hsu, C., & Backhouse, J. (2002). Information systems security education: Redressing the balance of theory and practice. *Journal of Information Systems Education, 13*(3), 211-218.

ISO/IEC 13888-3. (1997). *Information technology: Security techniques. Non-repudiation: Part 3. Mechanisms using asymmetric techniques.*

ISO/IEC 7498-2. (1988). *Information processing systems: Open systems interconnection. Basic reference model: Part 2. Security architecture.*

Lee, K. C., et al. (1997). Design and implementation of important applications in a Java-based multimedia digital classroom. *IEEE Transactions on Consumer Electronics, 43*(3), 264-270.

Lister, R., & Jerram, P. (2001). Design for Web-based on-demand multiple choice exams using XML. In *Proceedings of the IEEE International Conference on Advanced Learning Technology: Issues, Achievements and Challenges*, Madison, WI (pp. 383-386).

Pain, D., & Le Heron, J. (2003). WebCT and online assessment: The best thing since SOAP? *Educational Technology and Society, 6*(2), 62-71.

PGP. (n.d.). *The International PGP Home Page.* Retrieved from http://www.pgpi.org

Shafarenko, A., & Barsky, D. (2000). A secure examination system with multi-mode input on the World-Wide Web. In *Proceedings of the IEEE International Workshop on Advanced Learning Technology: Design and Development Issues (IWALT 2000)*, Palmerston North, New Zealand (pp. 97-100).

Shepherd, E. (2003, October 20). Delivering computerized assessments safely and securely. *The e-Learning Developers' Journal*, pp. 1-9.

Steinemann, M.-A., Zimmerli, S., Jampen, T., & Braun, T. (2002, May 20-22). Global architecture and partial prototype implementation for enhanced remote courses. In *Proceedings of Computers and Advanced Technology in Education (CATE 2002)*, Cancun, Mexico (pp. 441-446).

Sura, P. K., & Mukkamala, R. (2003, June 23-26). A PKI architecture for academic institutions: Design and prototype. In *Proceedings of the International Conference on Security and Management (SAM '03)*, Las Vegas, NV (Vol. 1, pp. 205-212).

Warren, M., & Hutchinson, W. (2003). Information security: An e-learning problem. In *Proceedings of the Second International Conference on Advances in Web-Based Learning (ICWL 2003)*, Melbourne, Australia (LNCS 2783, pp. 21-26).

World Wide Web Consortium (W3C). (2006). *Requirements for WCAG 2.0* (W3C Working Group Note).

Zhou, J. (2001). *Non-repudiation in electronic commerce.* Norwood, MA: Artech House Publishers.

Ana Isabel González-Tablas Ferreres received the engineer MSc degree from Universidad Politécnica de Madrid (Spain, 1999) and the PhD degree in computer science from Universidad Carlos III de Madrid (Spain, 2005). She has worked as a researcher and university assistant in Universidad Carlos III de Madrid since 1999. Her main research interests are security and privacy for location-based services and digital signature applications.

Agustín Orfila is a senior lecturer at the computer science department of the Universidad Carlos III de Madrid and a member of the Information Security Group of this department. He has a bachelor's degree in physics from Universidad Complutense de Madrid and he obtained his PhD degree in computer science from Universidad Carlos III de Madrid in 2005. Dr. Orfila has several publications in international conference proceeding and journals. His interests are mainly focused on the security of information technology, particularly on intrusion detection systems.

Benjamín Ramos Álvarez received the mathematics MSc degree and the computer science PhD degree from Universidad de Valencia (Spain, 1984) and from Universidad Carlos III de Madrid (Spain, 1999) respectively. Since 1990, he has been working in the computer sciences department at Universidad Carlos III de Madrid, currently as associate professor.

Arturo Ribagorda is a telecommunication engineer and PhD in computer science from the Polytechnical University of Madrid (SPAIN). At the moment he is full professor and head of the computer science department of the University Carlos III of Madrid (SPAIN). His research area is the security on information technology, field in which he worked in numerous research projects, national and international. He has published more than 40 papers in national magazines and international journals. He has been invited chair in numerous conferences and has written three books. In addition, he has been evaluator in European Research Programs (Advanced Transport Telematics and ESPRIT).