EVAWEB: A Web-Based Assessment System to Learn X.509/PKIX-Based Digital Signatures

Ana Isabel González-Tablas Ferreres, *Member, IEEE*, Karel Wouters, Benjamín Ramos Álvarez, and Arturo Ribagorda Garnacho

***Abstract*—EVAWEB is a Web-based assessment system that has been developed to evaluate the learning enhancement produced by the use of X.509 Public Key Infrastructure (X.509/PKIX)-based digital signatures in a real environment. EVAWEB allows the students to experience main X.509/PKIX processes related to the digital signature mechanism. In this paper, EVAWEB and its assessment by the students are described.**

***Index Terms*—Digital signatures, innovation in security teaching, Web-based assessment, X.509 Public Key Infrastructure (X.509/PKIX).**

I. Introduction

NOWADAYS, digital signatures, a kind of electronic analogue of handwritten signatures, are one of the core technologies in the information security field. Moreover, several European countries are deploying electronic identity cards, which allow the citizen to produce qualified signatures, legally equivalent to hand-written signatures [1]. Digital signatures are supported by public key certificates and Public Key Infrastructures (PKI). A public key certificate commonly means an electronic document that binds securely a public key with some identification. The most common public key certificate standard is the recommendation X.509, developed by the Telecommunication Standardization Sector of the International Telecommunication Union (ITU-T) [2]. A PKI provides the tools and operations that enable practical deployment of applications using public key certificates and, therefore, digital signatures. The Internet X.509 Public-Key Infrastructure (PKIX) Working Group within the Internet Engineering Task Force (IETF) is specifying a PKI for the Internet [3] using as base the ITU-T recommendation X.509. The whole set of PKIX documents is usually called the X.509/PKIX framework. The understanding of X.509/PKIX-based digital signatures and the tools which support them are crucial for students on information technologies and, to some extent, also for the general public.

ITIG10027—Security on Information Technologies (ITIG10027) is a mandatory course for third-year students of computer science engineering at *Universidad Carlos III de Madrid* in Spain. The total amount of hours assigned to the course is 75, 45 of them devoted to theory, and 30 to laboratory sessions.

The theory part of the course covers main aspects of security on information systems including security mechanisms, *malware* (malicious software), systems and physical security, security management, and legal aspects of security. Digital signatures and public key certificates are set out in the units related to security mechanisms and legal aspects of security.

A first block of laboratory sessions is devoted to carry out cryptography exercises including modular arithmetic, classical cryptography, symmetric and asymmetric modern encryption systems, hash functions, digital signature systems, and some simple cryptanalysis methods. In a second block of laboratory sessions, students must learn several security tools: Ethereal for network analysis, Aide for file system integrity verification, some simple rootkit software (a rootkit is a type of malicious software), Iptables and Snort as examples of firewall and intrusion detection systems, and the OpenSSL library and the Pretty Good Privacy (PGP) software as tools for computing hash functions, performing encryption and digital signatures, and managing public key certificates.

Motivation and goal—From the students' point of view, the curriculum content of the course ITIG10027 is huge and novel, which hinders the students from grasping it appropriately. To lessen students' efforts, the assessment method chosen by the teachers for the second block of laboratory sessions is to perform multiple-choice tests immediately after the sessions, so that the amount of work students must perform outside the sessions is reduced. However, this assessment approach does not favor a long-lasting learning.

In the last years, an increasing effort for innovating the teaching of information systems security has been noticed [4]. One of the approaches is to make the students practice in real or quasi-real environments, which in this case implies security risks. Furthermore, part of the academic community disapproves this approach because they believe that it educates hackers instead of security defenders. Despite difficulties and criticism, learning-by-doing in context stands as a successful educational theory in many study areas, and it is being integrated more and more in the teaching of information systems security [5].

The goal of the work presented in this paper is to evaluate how the use of the approach of learning-by-doing in context may enhance the students' learning of the X.509/PKIX framework and digital signatures based on it. To achieve this goal, 1) EVAWEB, which stands for "Sistema de EVAluación vía WEB" in Spanish

Manuscript received March 1, 2005; revised November 16, 2006. This work was supported in part by Universidad Carlos III de Madrid under the "1a CONVOCATORIA DE APOYO A EXPERIENCIAS DE INNOVACIÓN DOCENTE CURSO 2003–2004."

A. I. González-Tablas Ferreres, B. Ramos Álvarez, and A. Ribagorda Garnacho are with the Computer Science Department, Universidad Carlos III de Madrid, Leganés 28911, Madrid, Spain (e-mail: anaisabel.gonzalez-tablas@uc3m.es).

K. Wouters is with the ESAT/COSIC Research Group, K. U. Leuven, Leuven-Heverlee B-3001, Belgium (e-mail: Karel.Wouters@esat.kuleuven.be).

Digital Object Identifier 10.1109/TE.2007.893171

("Web-based assessment system" in English) that forces the students to use X.509/PKIX-based digital signatures, has been implemented; 2) EVAWEB has been evaluated by part of the students enrolled on ITIG10027.

Organization—In Section II, related work is analyzed. Section III describes EVAWEB and its intended use by the students to learn X.509/PKIX-based digital signatures. Finally, Sections IV and V present the assessment of the experience and the conclusions.

II. Related Work

Despite the risks involved in using X.509/PKIX-based digital signatures [6], they are being used in several electronic applications such as e-government, e-commerce, or e-Health [7]–[9]. Several researchers propose the use of PKI to solve most of the security problems in Higher Education [10]–[12]; some of them point out explicitly the use of this technology for providing nonrepudiation in electronic assessments [10]. However, despite PKI's advantages, deploying and maintaining such an infrastructure is a complex task, possibly being one reason that discourages the integration of digital signatures in e-learning environments or, at least, in e-learning tools. The authors are not aware of any e-learning tool that integrates X.509/PKIX-based digital signatures in Web-based on-line assessment.

One option to make students practice with X.509/PKIX-based digital signatures is to give them some naïve exercises, for example, using the OpenSSL tool. PGP is another framework that provides support for digital signatures, and it can also be used to teach digital signatures to the students [13]. However, PGP framework is used more for informal authentication, and it has not been widely deployed in real applications, such as e-government and e-banking, because of the Web-of-trust paradigm it relies on (different from the one used in the X.509/PKIX framework). Therefore, in the long term, learning X.509/PKIX-based digital signatures is more advantageous for the students.

The approach taken in this work is different from the usual approaches for teaching X.509/PKIX-based digital signatures in the sense that EVAWEB, the implemented system, provides a real environment that allows the students to experience most of the main processes defined in the X.509/PKIX framework and to use digital signatures with a real purpose and context.

III. Description of EVAWEB

EVAWEB is a Web-based assessment system that allows teachers to manage users (students and teachers), tests and question pools, and to generate the students' public key certificates. On the other hand, EVAWEB guides the students in some X.509/PKIX processes (signature key pair generation and public key certificate acquisition) and allows the students to perform Web-based tests and consult their grades. EVAWEB forces the students to sign the Web-based tests before submitting them to the server; in turn, EVAWEB returns the students a signed answer containing the grade. Each signed message can be used by the receiving party as non-repudiation evidence.

EVAWEB has a three-tier architecture deployed in a Web application server running on a servlet container (Tomcat 5) on the *server side* (Fig. 1) and a Web client (MSIE, Netscape, Firefox)

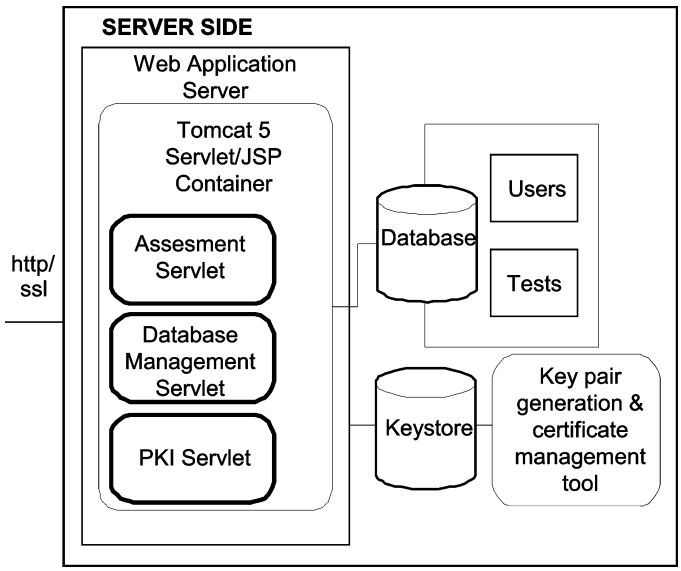

Fig. 1. Architecture of EVAWEB: server side.

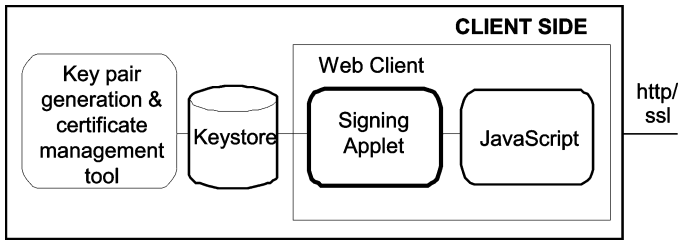

Fig. 2. Architecture of EVAWEB: client side.

supported by some processing capabilities on the *client side* (Fig. 2). In the following, EVAWEB architecture is briefly described; more details about the implementation can be found in [14], [15].

On the server side three main modules can be identified which 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 d*atabase 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. On the server side also a *database* exists containing users and tests information and a repository (*KeyStore*) containing the server signature keys and all the certificates.

On the client side, JavaScript is used to make 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 the browser via JavaScript.

In the following, how the X.509/PKIX framework is integrated in EVAWEB and the process that a student should follow to use the system are described.

A. Introduction to X.509/PKIX Framework

In public key cryptography, each user owns a pair of mathematically related keys called the public key and the private key. Although the public key is accessible by everyone, the private

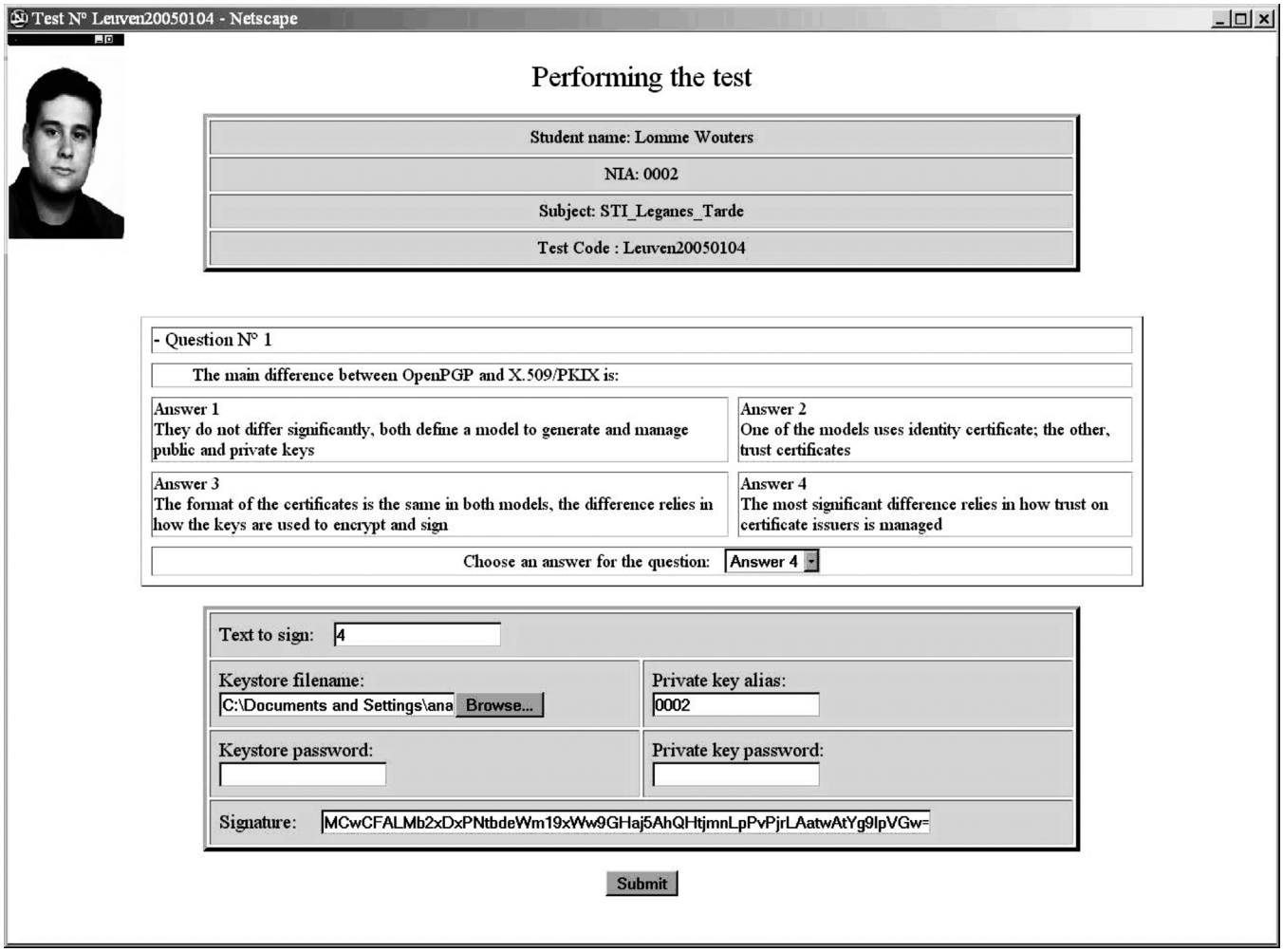

Fig. 3. An example of an answered and signed test (only one question).

key must be kept secret and be known only by the key pair owner. Digital signatures are generated using the private key and are verified using the public key. Signatures produced this way offer data origin authentication, entity authentication, and nonrepudiation.

Digital signatures must be supported by a trust model that securely binds some identification of the owner, such as an identity or a pseudonym, to the public key. The electronic document that ascertains the authenticity of the binding is called public key certificate. Certificates are issued by a trusted entity that is called *Certification Authority* (CA) in the context of the X.509/PKIX framework. A public key certificate comprises at least the public key, the identification of its owner, a period of validity, and the CA's digital signature over the previous data. To verify a signature, the verifier will first check the signature using the public key, then the validity status of the certificate (e.g., if it has been revoked).

In the X.509/PKIX framework several processes are specified. The main process is the *end entity certificate enrolment*, which results in the issuance of an end entity[1] public key certificate by the CA, and it is comprised by three steps: registration, initialization, and certification. Other main X.509/PKIX processes are the *certificate revocation request and certificate revocation list consultation*, by which an end entity requests a certificate revocation to make it invalid before its expiration date or consults which certificates have been revoked. This work focuses on the end entity certificate enrolment; in the following section how this process is integrated in EVAWEB is described.

[1]In EVAWEB scenario this entity is mainly the student.

B. End Entity Certificate Enrolment in EVAWEB

Registration. All students must enrol into the PKI before they can apply any of the enabled services. In EVAWEB this step occurs at the same time as the registration to the Web-based assessment system. The student is issued a shared secret that he/she must use for subsequent authentication as the enrolment process continues. As a requirement in EVAWEB, he/she must deliver also his/her digital photograph.

Initialization. In this step the student initializes the trust relation between him/her and the CA by following EVAWEB's instructions. The student uses a key generation tool to generate a key pair and the associated certificate request, which contains, among others, the public key. EVAWEB allows the student to submit the request to the CA and get the set of EVAWEB's certificates.

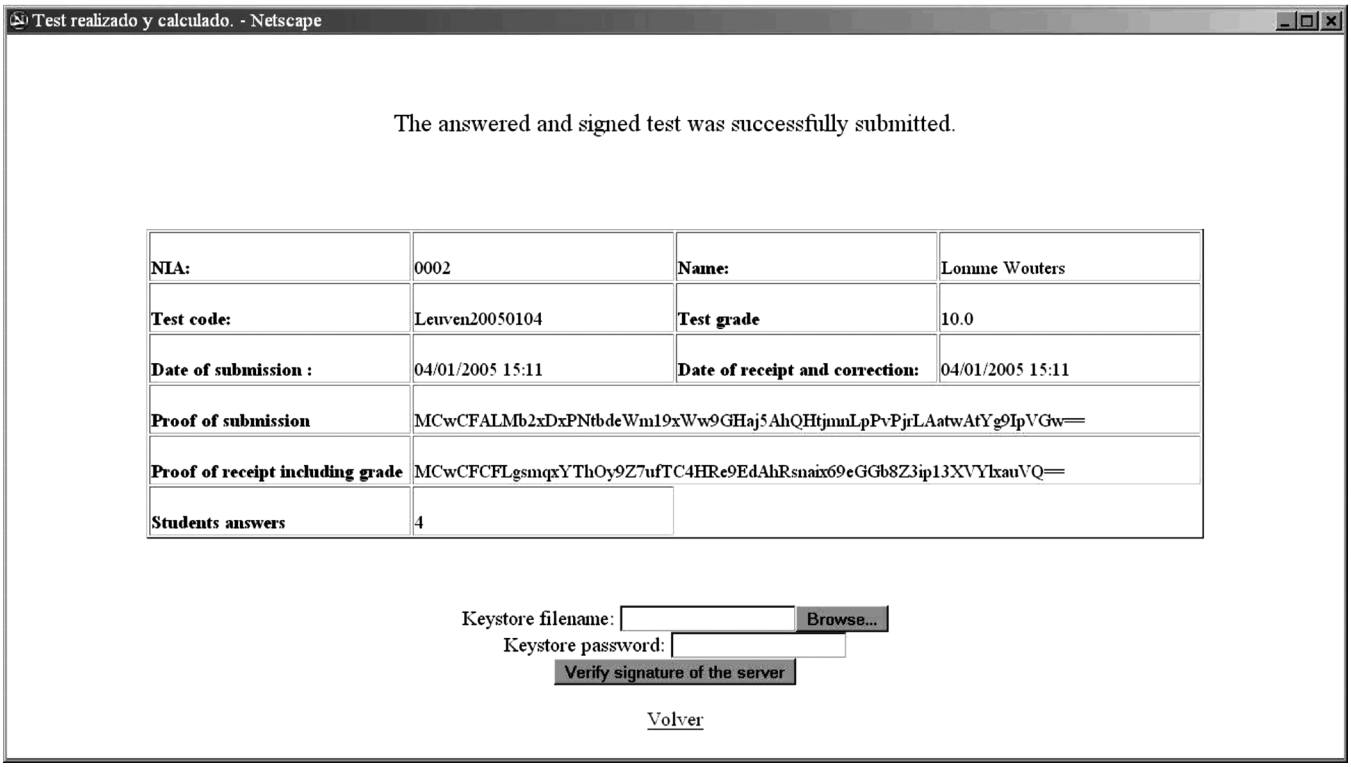

Fig. 4. Receipt of submission including grade.

Certification. The student's public key certificate is issued by the CA (the PKI servlet) and can be downloaded by the student from the repository.

C. Using X.509/PKIX-Based Digital Signatures in EVAWEB

After accessing the system, a student can choose to perform one of the available tests. To submit an answered test, students must first generate a signature on their answers and some other data (Fig. 3).

In EVAWEB, the signature is performed outside the Web browser by the signing applet. To generate the signature, first, the signed applet shows the student the answered test. Then, the student indicates where the private key is stored and types the passwords that protect the keystore and the key. Afterwards, 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/her assessment submission, including the grade (Fig. 4). The student can verify the server's signature and save the receipt.

IV. Evaluation

EVAWEB has been evaluated by an experimentation group of 28 volunteer students over the whole set of 83 students enrolled in the subject. Only 21 of the students in the group completed successfully the process of certification and assessment at least one of the three times they were asked. Besides, the students had to fill in the test on paper. At the end, the 28 students in the experimentation group were requested to evaluate the system by filling in an anonymous evaluation form. The most relevant questions contained in the evaluation form are presented in Table I, and statistics are presented in Table II.

Results in set (a) questions show that students evaluate Web-based assessment positively but do not completely trust this method using EVAWEB, because 46% of them do not agree on performing the tests using only the prototype (question a4). Students' fear is probably caused by the novelty of the system or by the preliminary state of the prototype. Results may have also been influenced by the seven students who never completed the tests.

Results of set (b) show that about 80% of the students agree on integrating digital signatures to provide nonrepudiation proofs of origin and receipt, respectively, for teachers and students (questions b1 and b2), but a slightly smaller percentage of about 70% (questions b3 and b4) considers that using the prototype helped him/her to better understand digital signatures and X.509/PKIX framework. An interpretation of the results of set (b) is that students assess the integration quite positively, but more work needs to be done to enhance EVAWEB's user-friendliness and usefulness for helping students to understand target technologies. In the evaluation of students' experience using the prototype in set (c), nearly 70% evaluate it positively and consider repeating the experience next year advantageous, in ITIG10027 and other subjects.

V. Conclusion

A main contribution of the research presented in this paper is the innovation in the teaching of X.509/PKIX-based digital

TABLE I
QUESTIONS IN THE EVALUATION FORM

(a) Web-based assessment
1. EVAWEB is adequate to assess this course's laboratory using Web-based tests.
2. EVAWEB enhances the previous paper-based assessment process because of automatic correction.
3. EVAWEB enhances the previous paper-based assessment process because of automatic feedback of the grade.
4. EVAWEB is adequate to perform ONLY Web-based tests (not both paper- and Web-based).
(b) Integration of digital signatures in Web-based assessment
1. It is adequate to integrate digital signature in Web-based assessment systems for issuing proofs of origin for teachers.
2. It is adequate to integrate digital signature in Web-based assessment systems for issuing proofs of receipt for students.
3. To use digital signatures integrated in Web-based assessment has helped me to understand this technology.
4.To use X.509 certificates and perform the related PKIX processes has helped me to understand this technology.
(c) Student experience
1. Has your experience in the evaluation of EVAWEB has been positive?
2. Would repeating the experience next year be adequate with students of this subject?
3. Would extending the experience to other subjects be adequate?

TABLE II
RESULTS OF THE EVALUATION (PERCENTAGES ARE ROUNDED).
(T = TOTAL, Q = QUITE, P = PARTIALLY, O = OTHERS)

Question %	Do not agree (-)			Do agree (+)				Cumulative	
	T	Q	P	P	Q	T	O	-	+
(a) Web-based assessment									
a.1)	0	14	14	21	39	11	0	29	71
a.2)	0	0	4	11	54	32	0	4	96
a.3)	0	0	4	11	50	32	4	4	92
a.4)	21	14	11	29	14	11	0	46	54
(b) Integration of digital signatures in Web-based assessment									
b.1)	4	4	7	18	32	32	4	14	82
b.2)	0	7	4	18	36	29	7	11	82
b.3)	0	7	18	25	36	11	4	25	71
b.4)	4	14	14	25	36	4	4	32	64
(c) Student experience									
c.1)	4	14	11	32	29	7	4	29	67
c.2)	0	14	4	14	39	29	0	18	82
c.3)	11	11	14	14	29	21	0	36	64

signatures. The goal was to enhance the students' understanding and learning of X.509/PKIX-based digital signatures by immersing them in an environment (learning-by-doing) where the use of this kind of signature is mandatory and has a real purpose. The chosen environment has been a Web-based assessment system, EVAWEB, which has been implemented to allow the evaluation of the learning-by-doing approach to teach X.509/PKIX digital signatures. Results show that the experience has been an above average success; some aspects must be enhanced, mainly the trust of students on EVAWEB and the pedagogical capabilities of the system.

In addition, the experience has led to some useful insights. EVAWEB has an integrated PKI that has to be deployed and maintained, not a straightforward task, requiring a great effort from the teachers. Furthermore, users must be strictly educated in the use of the PKI. This education should not be a problem if the users are students with a computer science background. However, if the use of the system is extended to other student profiles, the system must become more user-friendly and more effort be placed in user education. On the other hand, extending the use of the system to all students offers them a relatively simple environment for learning digital signatures in an easy way and becoming e-identity educated citizens.

Some future work can be identified such as enhancing the system's functionalities, improving usability and security, and increasing pedagogical capabilities. Furthermore, EVAWEB should be made modular (to integrate it easily with other Web-based e-learning systems) and compliant with existing e-learning and education standards. Integrating the system with an enhanced out-of-the box PKI with an LDAP repository [16] would be desirable, as would implementing the signature functionality on an electronic identity card. Experiments with students from nontechnical faculties should also be adopted. Finally, a proper study of the performance of EVAWEB should be completed, although both server and client performances have been acceptable during the evaluation (only 15 students using it simultaneously).

ACKNOWLEDGMENT

The authors would like to thank the referees of this paper for their constructive comments, B. Preneel for his valuable comments and suggestions, and the technical staff of the Laboratory of the Computer Science Department (Universidad Carlos III de Madrid) for their help and collaboration in the deployment and evaluation of the prototype.

D. Sánchez Torre and J. Rodríguez Gandía have implemented, respectively, first and second versions of EVAWEB, while being students of Universidad Carlos III de Madrid.

REFERENCES

[1] "Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a Community Framework for Electronic Signatures," 1999.

[2] "ITU-T Recommendation X.509: Information Technology—Open Systems Interconnection—The Directory: Authentication Framework," 2000.

[3] "RFC 3280, Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile," Apr. 2002.

[4] W. Yurcik and D. Doss, "Different approaches in the teaching of information systems security," in *Proc. 18th Annu. Information Systems Education Conf.—Technology in the 21st Century: Where Innovation and Information Converge*, Cincinnati, OH, Nov. 2001, §04a.

[5] C. Hsu and J. Backhouse, "Information systems security education: Redressing the balance of theory and practice," *J. Inf. Syst. Educ.*, vol. 13, no. 3, pp. 211–218, 2002.
[6] C. Ellison and B. Schneier, "Ten risks of PKI: What you're not being told about public key infrastructure," *Comput. Security J.*, vol. 16, no. 1, pp. 1–7, 2000.
[7] J. Claessens, V. Dem, D. De Cock, B. Preneel, and J. Vandewalle, "On the security of today's online electronic banking systems," *Computers and Security*, vol. 21, no. 3, pp. 257–269, 2002.
[8] R. Guida, R. Stahl, T. Bunt, G. Secrest, and J. Moorcones, "Deploying and using public key technology: Lessons learned in real life," *IEEE Security Privacy*, vol. 2, no. 4, pp. 67–71, 2004.
[9] M. Wimmer and B. von Bredow, "E-government: Aspects of security on different layers," in *Proc. 12th Int. Workshop Database and Expert Systems Applications*, Munich, Germany, 2001, pp. 350–355.
[10] PKI Applications in Academic Computing, 2001 [Online]. Available: http://www.cs.dartmouth.edu/~pkilab/acapps.shtml, Retrieved Jul 20, 2006 from Dartmouth PKI Lab Research Team's Web Page.
[11] M.-A. Steinemann, S. Zimmerli, T. Jampen, and T. Braun, "Global architecture and partial prototype implementation for enhanced remote courses," in *Proc. Computers and Advanced Technology in Education (CATE)*, Cancun, Mexico, May 2002, pp. 441–446.
[12] P. K. Sura and R. Mukkamala, "A PKI architecture for academic institutions: Design and prototype," in *Proc. Int. Conf. Security and Management (SAM'03)*, Las Vegas, NV, Jun. 2003, vol. 1, pp. 205–212.
[13] P. Zimmermann, *The Official PGP User's Guide*. Cambridge, MA: MIT Press, 1995.
[14] A. I. G.-T. Ferreres, K. Wouters, and B. R. Álvarez, "Teaching X.509/PKIX based digital signatures while enhancing non-repudiation of a web-based assessment system," in *Proc. IADIS Int. WWW/Internet Conf.*, Madrid, Spain, Oct. 2004, pp. 43–51.
[15] A. I González-Tablas Ferreres, A. Orfila Díaz-Pabón, B. Ramos Álvarez, and A. Ribagorda Garnacho, "EVAWEV v2: Enhancing a web-based assessment system," in *Proc. 4th Int. Conf. Multimedia and Information Communication Technologies in Education-Current Developments in Technology Assisted Education*, Sevilla, Spain, Nov. 2006, vol. 1, pp. 837–840.
[16] "RFC 4510, Lightweight Directory Access Protocol (LDAP): Technical Specification Road Map," Jun. 2006.

Ana Isabel González-Tablas Ferreres (M'05) received the M.Sc. degree in engineering from Universidad Politécnica de Madrid, Madrid, Spain, in 1999 and the Ph.D. degree in computer science from Universidad Carlos III de Madrid, Madrid, Spain, in 2005.

Since 1999, she has worked as a Research and Teaching Assistant at Universidad Carlos III de Madrid. Her main research interests are security and privacy for location-based services and digital signature applications.

Karel Wouters received the M.Sc. degree in mathematics from the Katholieke Universiteit Leuven, Leuven, Belgium, in 1997.

Since 1999, he has worked on several projects for the Computer Security and Industrial Cryptography (COSIC) Research Group at Katholieke Universiteit Leuven. His research interests include cryptography in and applied to XML, standards in cryptography, and document security.

Benjamín Ramos Álvarez received the M.Sc. degree in mathematics from Universidad de Valencia, Valencia, Spain, in 1984 and the Ph.D. degree in computer science and from Universidad Carlos III de Madrid, Madrid, Spain, in 1999.

Since 1990, he has worked in the Computer Sciences Department at Universidad Carlos III de Madrid. He is currently an Assistant Professor. His research is mainly focused in nonrepudiation issues of electronic signatures.

Arturo Ribagorda Garnacho received the M.Sc. degree in engineering in 1980 and the Ph.D. degree in computer science in 1983 from the Universidad Politécnica de Madrid, Madrid, Spain.

He is a Full Professor and Head of the Computer Science Department at Universidad Carlos III de Madrid, Madrid, Spain. His research is mainly focused on the security of information and communications technologies.