Security in Learning Management Systems: Designing Collaborative Learning Activities in Secure Information Systems

Authors

Jorge Miguel Moneo
jmmoneo@uoc.edu

Santi Caballé
scaballe@uoc.edu

Josep Prieto
jprieto@uoc.edu

Department of Computer Science Multimedia, and Telecommunication
Open University of Catalonia, Spain

Tags

learning management system, e-learning, information technology, information security, collaborative learning activities

The field of research on information technology applications in the design of computer supported collaborative learning (CSCL) activities generates very complex scenarios which must be studied from different approaches. One approach is to consider information security, but not only from a technological point of view.

In this paper we argue that current e-learning systems supporting on-line collaborative learning do not sufficiently meet essential security requirements, and this limitation can have a strong influence in the collaborative learning processes. In order to alleviate these problems we have proposed an approach based on Public Key Infrastructure (PKI) models that offer essential security properties and services in on-line collaborative learning, such as availability, integrity, identification and authentication, access control, confidentiality, non repudiation, time stamping, audit service and failure control.

1. Introduction

This paper proposes to emphasize information security issues when designing new e-leaning systems by incorporating security as an essential non-functional requirement into each and every collaborative learning process.

Information technology supported learning frameworks are present in the Spanish university system, where fully distance universities and virtual campuses exist, students do not only acquire knowledge and reinforce their educational skills and competences, but also learn to learn. Essential to attainment of this ideal is high quality materials that are carefully designed to be dynamic, intuitive and self-explanatory for students working within a distance education environment (Sangrà 2002).

All the actors implicated in on-line learning management systems demand increasingly specific requirements related to information security, in order to ensure the learning and teaching processes developed in this context and the information transmitted (Weippl 2005). However, when designing e-learning systems and applications, security is not a main concern and only conventional security methods and processes are considered in the requirements, such as authentication and basic authorization.

In this paper we argue that traditional security approaches when applied to the design of most advanced e-learning systems do not suffice to provide the necessary security requirements to guarantee that all supported learning processes are developed correctly and in a reliable way. The real learning context of this work is the Open University of Catalonia and the collaborative learning processes found as an essential part of the pedagogical model in all the on-line courses.

2. Background

Alan Bryden (2003), in his lecture "Open and Global Standards for Achieving an Inclusive Information Society" concerning the growth of the Information Society and its more equitable development, stated that the International Standards will greatly help to guarantee security and to develop consumer confidence and protection, while respecting the legitimate interests of all stakeholders.

As it could seem natural to follow these principles, international standards are still far from considering the essential role the security issues have in the learning processes and in the technology tools and systems supporting these processes. For instance, The IMS Global Learning Consortium has a series of reference specifications for e-learning but very few references regarding privacy and data protection: "While the details of the security architecture being employed to support the learner information system is outside the scope of this specification it is important to provide mechanisms that can be used to support the implementation of any suitable architecture" (IMS 2001).

El-Khatib (2003) examines privacy and security issues associated with e-learning, comparing how several learning standards consider the privacy security property. The conclusion in this paper is that current e-learning standards only treat privacy and security superficially, if at all.

Although privacy could be an important issue, what about the other ones? Is privacy service always really needed? For example, as an LMS offers course materials we could prefer public trusted materials to only private materials. Weippl (2005) states that "the goal of security in e-learning is to protect authors' e-learning content from copyright infringements, to protect teachers from students who may undermine their evaluation system by cheating, and to protect students from being too closely monitored by their teachers when using the software".

Since the above limitations and requirements are not met by existing e-learning systems, new approaches are needed.

3. Security in on-line collaborative learning: a first approach

Due Collaborative learning involves interactions, material management, communication processes and generation of learning results that should be supported in the LMS. Flate (2002) explains a LMS this way: Learning Management System is a broad term that is used for a wide range of systems that organize and provide access to online learning services for students, teachers, and administrators. These services usually include access control, provision of learning content, communication tools, and organizations of user groups.

The collaborative learning services are usually designed and implemented according to the needs of the collaborative learning model, without much consideration of security issues. This limitation may lead to undesirable situations that can influence the learning process and management, such as a student falsifying course materials, presenting a convincing false identity to other users, listening to private communications, altering the time stamp of assignments, and a teacher accessing students' personal data.

Current technological solutions based on Public Key Infrastructure (PKI) models are available to offer services which ensure the security properties and services so far. PKI, simply defined, is an infrastructure that allows the creation of a trusted method for providing privacy, authentication, integrity, and non-repudiation in communications between two parties (Raina 2003).

Grouping all the properties and security services needed, collaborative learning activities will be trusted if essential properties are reached, such as availability, integrity, identification and authentication, access control, confidentiality, non repudiation, time stamping, audit service and failure control (Shirey 2007).

PKI underlying infrastructure has techniques such as digital signature, digital certificates, certification authorities, and key stores, which form the system architecture to create security services ensuring all the properties compiled so far. Furthermore, PKI infrastructure adds specific services referred to in this paper such as time stamping. This service is essential in the development of collaborative learning activities when we need to verify the date or time of a transaction between the users of the LMS or an activity step.

4. Conclusions

In this paper we have argued that current e-learning systems supporting on-line collaborative learning do not sufficiently meet essential security requirements and this limitation can have a strong influence in the collaborative learning processes. In order to alleviate these problems we have proposed an approach based on Public Key Infrastructure (PKI) models that offer services which ensure essential security properties and services in on-line collaborative learning, such as availability, integrity, identification and authentication, access control, confidentiality, non repudiation, time stamping, audit service and failure control.

Acknowledgements

This work has been supported by the European Commission under the Collaborative Project ALICE ”Adaptive Learning via Intuitive/Interactive, Collaborative and Emotional System”, VII Framework Programme, Theme ICT-2009.4.2 (Technology-Enhanced Learning), Grant Agreement n. 257639.

References

Bryden, A., 2003. Open and Global Standards for Achieving an Inclusive Information Society. In SIST Conference. Ljubljana, Slovenia. Available at: http://www.iso.org/iso/livelinkgetfile?llNodeId=21921&llVolId=-2000.

El-Khatib, K. et al., 2003. Privacy and Security in E-Learning. *International Journal of Distance Education*, 1(4).

Flate, M., 2002. Online Education Systems: Discussion and Definition of Terms. NKI Distance Education. Available at: http://www.porto.ucp.pt/open/curso/modulos/doc/Definition%20of%20Terms.pdf.

IMS, 2001. Final Specification of IMS Learner Information Package Information Model. Available at: http://www.imsglobal.org/profiles/lipinfo01.html.

Raina, K., 2003. PKI security solutions for the Enterprise : solving HIPAA, E-Paper Act, and other compliance issues, Indianapolis, Ind: Wiley Pub.

Sangrà, A., 2002. A New Learning Model for the Information and Knowledge Society: The case of the Universitat Oberta de Catalunya (UOC). International Review of Research in Open and Distance Learning. Available at: http://www.irrodl.org/index.php/irrodl/article/view/55/114.

Shirey, R., 2007. RFC 4949: Internet Security Glossary, Version 2. Available at: http://tools.ietf.org/html/rfc4949.

Weippl, E.R., 2005. Security in e-learning, New York, NY: Springer.

Edition and production

Name of the publication: eLearning Papers
ISSN: 1887-1542
Publisher: elearningeuropa.info
Edited by: P.A.U. Education, S.L.
Postal address: c/Muntaner 262, 3r, 08021 Barcelona (Spain)
Phone: +34 933 670 400
Email: editorial@elearningeuropa.info
Internet: www.elearningpapers.eu

Copyrights

SOME RIGHTS RESERVED

The texts published in this journal, unless otherwise indicated, are subject to a Creative Commons Attribution-Noncommercial-NoDerivativeWorks 3.0 Unported licence. They may be copied, distributed and broadcast provided that the author and the e-journal that publishes them, eLearning Papers, are cited. Commercial use and derivative works are not permitted. The full licence can be consulted on http://creativecommons.org/licenses/by-nc-nd/3.0/

View publication stats