

Development of E-Learning Design Criteria with Secure Realization Concepts

Christian J. Eibl, Sigrid E. Schubert
Didactics of Informatics and E-Learning, University of Siegen
Hölderlinstr. 3, D-57076 Siegen, Germany
{eibl | schubert}@die.informatik.uni-siegen.de

Summary

Information security is a major quality factor for informatics systems and essential for enduring web-based offerings like e-learning. The term e-learning is used in practice in many different ways such that in parts even simple web pages with downloadable files like lecture notes are considered as e-learning. To get a definition of well acceptable and facilitating e-learning systems really focusing on the learning process, the underlying research project, first, investigates requirements from affiliated disciplines like educational science. This resulted in demands for equal opportunities (A1), social support by co-operation and communication facilities (A2), activities of students as important steps of the learning process (A3), priority to meet learning objectives (A4), flexible learning with sufficient adaptability to different target groups (A5), and integration of e-learning in an existing learning environment (A6). Since every criterion applied in implementing such a system increases the system's complexity, this undoubtedly leads to further demands for information security investigation to meet newly emerging security issues. Hence, to manage this complexity resp. high complex software creation in general aspects of the research field of software engineering are included in the examination of design criteria for e-learning.

Demands stated by software engineering are mostly focusing on good software quality which can be classified in a structured set of criteria and sub-criteria as follows: functionality (B1), reliability (B2), usability (B3), efficiency (B4), maintainability (B5), and portability (B6). Especially usability and functionality demands are important for not restraining learners in their learning process and provide them with an easy to use interface, such that interactions with the learning system are possible without distracting them by technical issues. Maintainability and portability give options to adapt the system appropriately to different target groups and allow reactions to changing infrastructures.

Considering privacy aspects like learning process and progress as well as personal data like different kinds of relations among learners, it gets obvious that security aspects must be considered accordingly. In this research project we consider e-learning systems to be secure if they guarantee availability (C1), integrity (C2), and confidentiality (C3) for authorized users where all of these aspects are given with respect to sufficient access control mechanisms (C4). These aspects must be managed from a technical point of view, e.g., for an appropriate infrastructure with sufficient control and detection mechanisms, as well as from an organizational point of view where privileges are assigned according to planned activities of different roles in the system.

Based on interdisciplinary requirements of education and informatics we propose a theoretical realization of design criteria of appropriate security architectures and give a prototype for the practical realization of all stated criteria in form of a proxy server for automated security processes in the learning management system "Moodle". This proxy server demonstrates the feasibility of stated concepts and enables outsourcing of security-related tasks, i.e., automate such processes without further user interaction. Although the current prototype shows the feasibility of applying and implementing stated design criteria, further research is necessary to firm up relevant criteria for necessary parts of a learning environment integrating e-learning.