Chapter 65
Architecture of Combined E-Learning Environment and Investigation of Secure Access and Privacy Protection

Radi Romansky
Technical University of Sofia, Bulgaria

Irina Noninska
Technical University of Sofia, Bulgaria

ABSTRACT

The contemporary digital world based on network communications, globalization and information sharing outlines new important targets in the area of privacy and personal data protection which reflect to applied principles of secure access to proposed information structures. In this reason the aim of secure access to all resources of an e-learning environment is very important and adequate technological and organizational measures for authentication, authorization and protection of personal data must be applied. Strong security procedures should be proposed to protect user's profiles, designed after successful registration and all personal information collected by educational processes. The goal of this article is to present an idea to combine traditional e-learning technologies with new opportunities that give mobile applications, cloud services and social computing. These technologies can endanger data security since they make possible remote access to resources, sharing information between participants by network communications. In order to avoid data vulnerabilities users must be identified and authenticated before, i.e. to be allowed to access information resources otherwise integrity and confidentiality of e-learning system could be destroyed. In order to propose solution basic principles of information security and privacy protection in e-learning processes are discussed in this article. As a result, an organizational scheme of a system for information security and privacy is proposed. Based on these principles a graph formalization of access to the system resources is made and architecture for combined (heterogenic) e-learning architecture with secure access to the resources is designed. Analytical investigation based on designed Markov chain has been carried out and several statistical assessments delivered by Develve software are discussed.

DOI: 10.4018/978-1-5225-7113-1.ch065

INTRODUCTION

E-learning is an important part of contemporary Information Society and all initiatives of the European Commission (EC) from the beginning of current century are focused on e-learning systems' development. The global network Internet proposes many opportunities for collaboration and remote access, making communications easy and fast. Implementation of cloud and social computing technologies contribute to the success of the understanding and accepting of e-learning policy as a whole (Peytcheva-Forsyth, 2015). There are different proposals for e-learning architectures based on cloud services and social media (Joshi, 2014; Masud, 2012, Velicanu, 2013, Neville, 2013). These new technologies have many advantages which sometimes could cause difficulties with protection of information resources and personal data (Romansky, 2014) collected and processed during e-learning procedures (Chen, 2013).

The Web applications which usually share personal information, determine a necessity for secure Internet connections, hence network providers must guarantee user's privacy (Fisher, 2014; Kinast&Partner, 2014). It is well known that the privacy is a fundamental human right and it very often depends on secure processing of personal data. Different components of the digital word require creation of personal profiles that consist of personal data and they should be protected by improving the legislation (Shear, 2013) and by ensuring adequate level of security (Symantec, 2014). In this reason the European Commission has proposed a new regulation in the field of privacy in the cyber space and has promoted the new paradigm "right to be forgotten / to be erased" (European Commission, 2014).

Different models and schemes for digital education are used as basic components of contemporary digital world and all aspects of digital privacy and secure access to the profiles with personal data must find adequate solution. At present day e-Learning environments are extended by opportunities that give social computing (Neville, 2013; Rotkrantz, 2015) and cloud services (Velicanu, 2013) which outline new challenges for digital privacy (Fisher, 2014; Kinast&Partner, 2014; Taylor, 2013). Different techniques for investigation of e-learning approaches, able to validate secure e-learning schemes are used. Some of the most popular methods are graph formalization (Sun, 2014), statistical modelling (Nouri, 2014), stochastic modelling (Abraham, 2014), etc. The Markov chain theory is defined as one of well applicable apparatus for investigation of processes in e-learning structures (Taraghi, 2014a; Taraghi, 2014b).

This article is extended and renewed version of (Romansky, 2015a) and discuses basic security measures and privacy rules in e-learning environment and presents an idea for organization of a complex e-servicing system with internal educational resources and remote access to external educational space based on cloud and social computing technologies. The proposed structure unites two sub-systems where functions for security and privacy protection are divided (Romansky, 2015b): *Front office* is designed for user's authentication and personal profiles creation; *Back office* is responsible for access control based on authorization, digital rights management and personal data protection. A preliminary conceptual defining is made and a formalization of components of the proposed combined e-learning environment by using state transition network (STN) is realized (Romansky, 2015c). A Markov model for investigation of processes in this heterogenic e-learning environment is designed. This model is used for components' assessment, where special attention on processes of authentication and authorization of the users is paid. Investigation is extended by statistical analysis of calculated probability sets by using the "Develve" software (http://develve.net/).