Chapter 1.12
Privacy and Security in E-Learning[1]

George Yee
Institute for Information Technology, Canada

Yuefei Xu
Institute for Information Technology, Canada

Larry Korba
Institute for Information Technology, Canada

Khalil El-Khatib
Institute for Information Technology, Canada

ABSTRACT

For a variety of advantages, universities and other organizations are resorting to e-learning to provide instruction online. While many advances have been made in the mechanics of providing online instruction, the needs for privacy and security have to-date been largely ignored. This chapter examines privacy and security issues associated with e-learning. It presents the basic principles behind privacy practices and legislation. It investigates the more popular e-learning standards to determine their provisions and limitations for privacy and security. Privacy requirements for e-learning systems are explored with respect to the "privacy principles." The capabilities of a number of existing privacy enhancing technologies, including methods for network privacy, policy-based privacy/security management, and trust systems, are reviewed and assessed.

INTRODUCTION

One of the key characteristics of our information economy is the requirement for lifelong learning. Industrial and occupational changes, global competition, and the explosion of information technologies have all highlighted the need for skills, knowledge, and training. Focused on attracting and retaining staff, companies have placed an emphasis on training to bolster soft and hard skills to meet new corporate challenges. In many cases, career training has been placed in the hands of employees, with the understanding that employees must be able to keep ahead of technological change and perform innovative problem solving. One way of meeting the demand for these new skills (especially in information technology) is through online e-learning, which also offers the potential for continuous learning. Moreover, e-learning provides answers for the rising costs of tuition, the shortage of qualified training staff, the high cost of campus maintenance, and the need to reach larger learner populations.

From the corporate perspective, employee training is an approach to increase the level and variety of competencies in employees, for both hard and soft skills. Online learning has become an important tool to implement corporate learning objectives. Indeed, specific e-learning courseware may be used to target specific corporate needs pertaining to strategic directions. Key trends for corporate e-learning, germane to privacy and e-learning include (Hodgins, 2000):

- Learners may access courseware using many different computing devices and from different locations, via different networks.
- E-learning technology will overtake classroom training to meet the needs for "know what" and "know how" training.
- E-learning will offer more user personalization, whereas courseware will dynamically change based on learner preferences or needs. In other words, e-learning applications of the future will be intelligent and adaptive.
- Corporate training is becoming knowledge management. This is the general trend in the digital economy. With knowledge management, employee competencies are assets which increase in value through training. This trend has pushed the production of training that is more task specific than generic. Changes in corporate strategic directions are often reflected as changes in e-learning requirements prompted by the need to train staff for those new directions.
- E-learning is moving toward open standards.

Most e-learning innovations have focused on course development and delivery, with little or no consideration to privacy and security as required elements. However, it is clear from the previous trends that there will be a growing need for high levels of confidentiality and privacy in e-learning applications, and that security technologies must be put in place to meet these needs. The savvy of consumers regarding their rights to privacy is increasing, and new privacy legislations have recently been introduced by diverse jurisdictions. It is also clear that confidentiality is vital for information concerning e-learning activities undertaken by corporate staff. While corporations may advertise their learning approaches to skills and knowledge development in order to attract staff, they do not want competitors to learn the details of training provided, which could compromise their strategic directions.

In this chapter, we investigate the problem of privacy and security for distributed mobile e-learning systems. These kinds of e-learning systems provide service mobility, where the learner can access the learning content from anywhere using any suitable device (e.g., desktop computer at home or work, PDA with wireless connection). We focus on the protection of personal information of a learner in an e-learning system. While it is an

Related Content