A Study on User's Perception in E-learning Security and Privacy Issues

Madeth May
University of Lyon
Industrial Engineering Department
19, avenue Jean Capelle, Villeurbanne F-69621, France
madeth.may@insa-lyon.fr

Georgios Fessakis
University of Aegean
LTEE Laboratory
1 av. Democratias, Rhodes 85100, Greece
gfesakis@rhodes.aegean.gr

Angelique Dimitracopoulou
University of Aegean
LTEE Laboratory
1 av. Democratias, Rhodes 85100, Greece
adimitr@aegean.gr

Sébastien George
University of Lyon
LIRIS laboratory, INSA-Lyon
7 avenue Jean Capelle, Villeurbanne F-69621, France
sebastien.george@insa-lyon.fr

Abstract—**Researchers have proven with both theoretical and empirical studies that technologies could enhance learning. Meanwhile, technologies could also create barriers to the latter. Particularly, when the use of technologies causes security and privacy concerns, E-learning becomes less fruitful as the participants are too afraid to be exposed by what has been provided to help them learn in the first place. This paper presents a study on user's perception in using E-learning technologies and the relevant issues. The major contribution of this paper is the awareness-raising of security and privacy issues, which are often overlooked in the research efforts that implicate user tracking and personal data usage for instructional purposes.**

Keywords-E-learning; tracking system; tracking data; security and privacy concern

I. INTRODUCTION

Within the past five years, we witness a strong growth of research efforts which aim at developing technologies that better support user participation and interactivity while others attempt to provide new technological approaches, such as "user tracking", to make online learning and teaching easier and more efficient in terms of student monitoring and evaluation [1]. In fact, using tracking approaches in E-learning has been proven to be a reliable support to both teachers and students. It is also recognized as a major contributing factor to high quality teaching and learning guidance [2]. For example, thanks to the tracking systems integrated in learning platforms, teachers can keep themselves informed of the activities being undertaken by the students. As for the students, having records of their activities help them keep tracks of their personal progress, their exchanges among other students and their achievements throughout the learning session. Therefore, E-learning tracking data have become significant sources of information that reveal both the users' activities and their outputs [3]. Those data can be exploited not only by teachers and students, but also by researchers and developers of learning technologies. Using tracking systems has been done in numerous ways in E-learning in accordance with the technological progress being made. In the meantime, it has increased security and privacy problems, which lead to a situation where security and privacy protection are becoming essential for the users.

II. RESEARCH OVERVIEW

Our research focuses on the Computer Mediated Communications (CMC). While CMC tool is recognized as an essential element to E-learning and is strongly recommended for the participants [4], there are still issues that we should recognize. If we take a closer look at the use of CMC tool in E-learning, CMC tool alone does not always enable the participants to fully control their activities the way they do in a traditional face-to-face learning situation. Having studied some issues, we addressed the importance of tracking CMC in learning situations for the benefits of tracking data to online tutoring and learning enhancements. An explicit tracking approach has been proposed for the implementation of tracking systems for a great variety of CMC tools [5]. It focuses on a tracking mechanism capable of observing different types of user action and interaction on CMC tools. Later, we continue our research by focusing on exploiting the collected data to support the participants in terms of gaining awareness and making assessment of their learning activities, outcomes and effectiveness [6].

III. SECURITY AND PRIVACY ISSUES IN E-LEARNING

Privacy issues concern learning technology providers, learning service and content providers, and the participants themselves. Indeed, the crucial tasks for learning service and content providers are to secure learning environment and to secure storage of learner data. As for the participants, they are mainly concerned with trust assessment of learning environments they are using, and with protection of their sensitive personal data [7].

Security and privacy levels differ in various learning environments and depend on types of learning activities being conducted by the participants. To have quick overview of some issues of privacy and security in learning technology as well as learners and their protection provisions, we look at some research data taken from [8] and [9]. A survey has been conducted to study the urgency of different protection. A total of 147 people responded to a questionnaire, among which 66% represented universities and higher educational institutions. 67 participants are learning technology and service providers, 38 are learning content providers, and 42 are end-user organizations. The synthetic results are presented in figure 1.

	Non relevant	Nice to have	Relevant	Urgent	Very urgent	I don't know	No answer
Protection of personal data	0%	9%	36%	31%	24%	1%	0%
Anonymous use	10%	16%	45%	23%	6%	1%	0%
Address and location privacy	5%	10%	37%	22%	22%	1%	2%
Single sign-on	3%	12%	37%	26%	16%	2%	5%
Seamless access	1%	10%	33%	33%	17%	1%	5%
Authenticity of LRs	2%	14%	25%	32%	24%	1%	2%
Digital Rights Management	15%	11%	33%	25%	16%	0%	0%
Legislation	7%	13%	52%	18%	5%	1%	3%
Awareness raising	5%	10%	26%	24%	33%	1%	2%

Figure 1. Urgency of protection measures.

Interesting information can be retrieved from figure 1. Examples include user data protection and anonymity that are strongly relevant to privacy concern in learning environment. Besides personal data protection, students requested to be able to control the visibility of their sensitive data such as history of their learning activities and their profiles. That is why various privacy-enhancing technologies are proposed by [10] and [11] for privacy protection at both learner side and provider side. Those technologies include identity protectors, anonymous communication systems and cryptographic mechanisms.

IV. A Broader Perspective on the Studied Issues

To get the better of privacy concerns is not only about using technological solutions to keep users safe from any threats, but also about "trust". Trust is a crucial enabler for meaningful and mutually beneficial interactions that build and sustain learner collaboration and community [7]. As yet, privacy is a natural concern at the same time that trust is an important factor in learning environment because in practice, privacy and trust are circularly related. In reality, in a closed learning environment, where all learning services are provided internally (e.g. from a university or a trusted source) students can have higher confidence that their personal data will be treated properly. On the other hand, in an open learning environment with unknown providers such as private or external learning service providers, privacy concerns are higher and the trust level of learners will be influenced by the level of perceived privacy offered by those providers.

From a technological perspective, the solution to the security and privacy issues is still heavily reliant on technological approaches. From a researcher in E-learning perspective, what is important is the fact that student's personal data benefit from any type of exposure in any circumstance. Nevertheless, a compromise between tracking students and protecting their privacy is still needed. For example, allowing students to anonymously access to their learning environments for a privacy reason is feasible from a technological standpoint, but somehow limited from the fact that a learning application aims at assisting students and so they cannot act in full anonymity.

V. Conclusions

To conclude, technologies such as user tracking should not be seen as a threat to the users as long as (i) they are informed of any tracking process when they access learning platforms and (ii) only on their approval that any tracking process can take place. Throughout our research efforts, there is always an acknowledgement from our part on the protection of users' personal data and their entity privacy.

References

[1] R. Mazza and L. Botturi, "Monitoring an Online Course with the GISMO Tool: A Case Study," International Journal of of Interactive Learning Research, vol. 18, no. 1, pp. 251-265, 2007.

[2] P. Jermann, A. Soller, and M. Muehlenbrock, "From Mirroring to Guiding: A Review of State of the Art Technology for Supporting Collaborative Learning," in Proceedings of the First European Conference on Computer-Supported Collaborative Learning, Maastricht, The Netherlands, 2001, pp. 324-331.

[3] M. May, S. George, and P. Prévôt, "A Closer Look at Tracking Human & Computer Interactions in Web-Based Communications," International Journal of Interactive Technology and Smart Education, vol. 5, no. 3, pp. 170-188, 2008.

[4] Z. Berge and M. Collins, "Computer-Mediated Communication and the Online Classroom in Distance Learning," Computer-Mediated Communication Magazine, vol. 2, no. 4, p. 6, 1995.

[5] M. May, S. George, and P. Prévôt, "Students' Tracking Data: an Approach for Efficiently Tracking Computer Mediated Communications in Distance Learning," in IEEE 8th International Conference on Advanced Learning Technologies, Santander, France, 2008, pp. 783-787.

[6] M. May, S. George, and P. Prévôt, "TrAVis to Enhance Online Tutoring and Learning Activities: Real Time Visualization of Students Tracking Data," in IADIS International Conference on E-learning, Freiburg, Germany, 2010, pp. 57-64.

[7] M. Anwar and J. Greer, "Reputation Management in Privacy-enhanced E-learning," in Proceedings of the 3rd Annual Scientific Conference of the LORNET Research Network, Montreal, Canada, 2006, p. 6 pages.

[8] T. Klobucar, M. Jenabi, A. Kaibel, and A. Karapidis, Security and Privacy Issues in Technology Enhanced Learning, ISO Press. Amsterdam: IOS Press, 2007.

[9] M. Wolpers and G. Grohmann, "PROLEARN: Technology Enhanced Learning and Knowledge Distribution for the Corporate World," International Journal of Metadata, Semantics and Ontologies, vol. 1, no. 1, pp. 44-61, 2005.

[10] V. Senicar, B. Jerman-Blazic, and T. Klobucar, "Privacy Enhancing Technologies – approaches and development. Computer Standards & Interfaces," Computer Standards & Interfaces, vol. 25, no. 2, pp. 147-158, 2003.

[11] K. El-Khatib, L. Korba, Y. Xu, and G. Yee, "Privacy and Security in E-Learning," International Journal of Distance Education, vol. 1, no. 4, p. 16 pages, 2003.