Enforcing privacy for teenagers in online inquiry learning spaces

Na Li, Adrian Holzer, Sten Govaerts, Denis Gillet

Enforcing Privacy for Teenagers in Online Inquiry Learning Spaces

Na Li
École Polytechnique Fédérale de Lausanne (EPFL)
1015 Lausanne, Switzerland
na.li@epfl.ch

Adrian Holzer
École Polytechnique Fédérale de Lausanne (EPFL)
1015 Lausanne, Switzerland
adrian.holzer@epfl.ch

Sten Govaerts
École Polytechnique Fédérale de Lausanne (EPFL)
1015 Lausanne, Switzerland
sten.govaerts@epfl.ch

Denis Gillet
École Polytechnique Fédérale de Lausanne (EPFL)
1015 Lausanne, Switzerland
denis.gillet@epfl.ch

Abstract
In the Go-Lab European project, we are investigating an online lab portal that enables students to perform personalized scientific experiments with online labs. To protect sensitive student data, such as user activity data and learning preferences, this paper presents a classroom-like pseudonymity approach that fulfills the specific requirements of the Go-Lab portal: (1) enforcing student privacy, (2) enabling personalization, and (3) providing a teenager-friendly design.

Author Keywords
Privacy, anonymity, identity, teenagers, online labs, user experience

ACM Classification Keywords
H.5.0 [Information interfaces and presentation]: General.

General Terms
Design, Human Factors

Introduction
In the *Go-Lab*[1] European project, we are creating an online lab portal that enables students (from 10 to 18 years old) to perform personalized scientific experiments with online labs, and offers teachers the opportunity to

[1] Go-Lab project: http://www.go-lab-project.eu

enrich their classroom activities by using pedagogically structured Web-based Inquiry Learning Spaces [3], (referred to as ILS hereafter).

An ILS is an online space created or adapted by a teacher for an inquiry learning [2] activity for students. A typical ILS contains online labs, learning resources, and apps that support the inquiry learning activities. The Go-Lab portal consists of three components [4]: *ILS repository*[2] where teachers can search and browse online labs and sample ILSs created by others, *ILS editor* built upon the *Graasp*[3] [1, 5] platform where teachers can construct and modify their own ILSs, and *ILS student view* where the students can access and perform scientific experiments. In this paper, we focus on the design of a teenager-friendly privacy mechanism for the *ILS student view*.

On one hand, an ILS aims at providing students with personalized learning experiences, which requires tracking of students' activities. On the other hand, such information reveals the learning preferences and learning progresses of students, thus it should not be exposed to anyone outside the classroom. In this paper, we present a classroom-like pseudonymity approach to overcome the tension between sensitive data protection and learning experience personalization.

The requirements

To properly handle the student privacy issue, we first need to understand the specific privacy requirements of the *ILS student view*. Three key requirements are summarized as follows:

- *Preserving student privacy.* In a real-life classroom, the learning traces left behind by students are accessible to the teacher, but should not be exposed to anyone outside the classroom such as other teachers, the platform provider, and analytics engines. Within an ILS, we aim to achieve a similar privacy setting, where the teacher and students can be aware of each other's activities but anyone outside of the classroom should not be able to identify student activity.
- *Enabling personalization.* The Go-Lab portal will provide personalisation to students and teachers. For instance, based on the student behavior while conducting an experiment, the system could provide personalized hints to guide the inexperienced students. Therefore, the privacy solution should allow personalization while preserving an appropriate level of privacy for the students.
- *Providing a teenager-friendly design.* Students will use the online labs and ILS under the teacher's guidance. The privacy mechanism should be straightforward, and the corresponding user interface should be easy to use for teenagers.

Various identity schemes have been used in different systems to fulfill their specific privacy requirements. Table 1 illustrates the fit between different identity approaches and the requirements of the Go-Lab portal. Full identity such as email-based registration and login allows personalization because users' actions can be fully tracked and identified. However, it does not protect users' privacy since their personal information is disclosed to the platform provider. Moreover, full identity requires users to go through a signup process and provide username and password upon login, which increases the entry barrier.

[2] Go-Lab repository: http://golabz.eu
[3] Graasp: http://graasp.epfl.ch

Although anonymity ensures privacy for users and provides easy access, it hinders personalization as the tracked behavior of anonymous users can not be identified. An example of such an anonymity approach is Google Drive, which allows users to access a shared document via a secret link without sign-in.

In the Go-Lab project, the anonymity approach is used in the *ILS repository* where teachers can search and browse the sample ILSs anonymously without sign-in. An email-based full identity scheme is employed in the *ILS editor* where teachers can log in and create their ILSs. To fulfill all the requirements of the *ILS student view*, we propose a *classroom-like pseudonymity* approach that follows the privacy paradigm of real-life classrooms.

Table 1: Fit between different identity approaches and the requirements of the Go-Lab portal.

Requirements	Full Identity	Anonymity	Classroom-like Pseudonymity
Privacy	-	+	+
Personalization	+	-	+
Ease of use	-	+	+

The approach

After a teacher logs in the *ILS editor*, she can create an ILS. For each ILS, the system generates a unique secret URL which the teacher shares with the students and allows just the students to access the ILS. Additionally, the teacher can specify an expiry date to limit access within a given period of time, e.g. a semester.

To lower the entry barrier but still enable personalization, the *ILS student view* requires neither login nor user registration process, but a unique nickname. When accessing the *ILS student view*, a student is asked to provide a nickname to identify herself. This nickname should be unique within the scope of the ILS. More specifically, the identity of the student can be described by a 3-tuple (N, S, T), where N denotes the nickname of a student, S denotes the ILS that the student accesses, and T denotes the time period within which the secret URL of the ILS is valid.

As only the teacher knows about the mapping between the nickname and the student, she can keep track of each student's learning progress (e.g. using learning analytics techniques) while this information is not disclosed to anyone outside the ILS. Such an approach is consistent with the privacy paradigm in a real-life classroom where the teacher can observe the student activities and adjust the learning process accordingly. Furthermore, the student behavior can be tracked with this identity and provide personalized guidance and awareness cues. The nickname improves usability since it enables teacher and students to relate tracked activity to a specific person. For instance, the ILS can preserve a particular student's current progress so that the student can resume her activity next time she accesses the ILS and can highlight who contributed what with the nickname. Finally, the registration and login hassle is eliminated for students.

The implementation

This section details the current implementation of the proposed privacy mechanism. To carry out an inquiry learning activity in the classroom, the teacher sets up in advance an ILS. Figure 1 illustrates an example ILS created for a lecture on galaxy collisions. Learning resources and apps are added in the ILS to help students understand and simulate how galaxies form and evolve.

During the lecture, the teacher shares the secret URL of the ILS with her students. Then, each student accesses the secret URL, which opens the *ILS student view*, as illustrated in Figure 2. After providing a nickname in the pop-up window, each student can log in and perform the experiment according to the teacher's instructions.

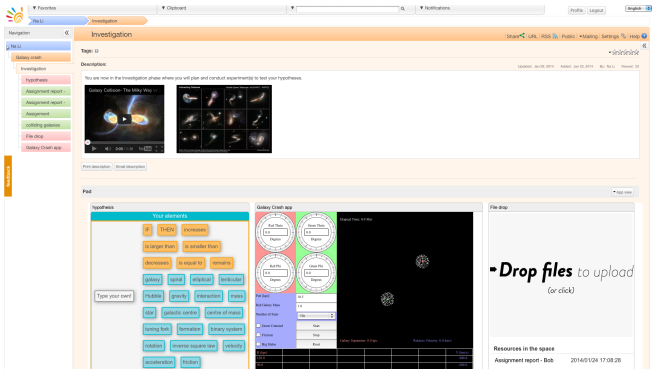

Figure 1: User interface of the *ILS editor*.

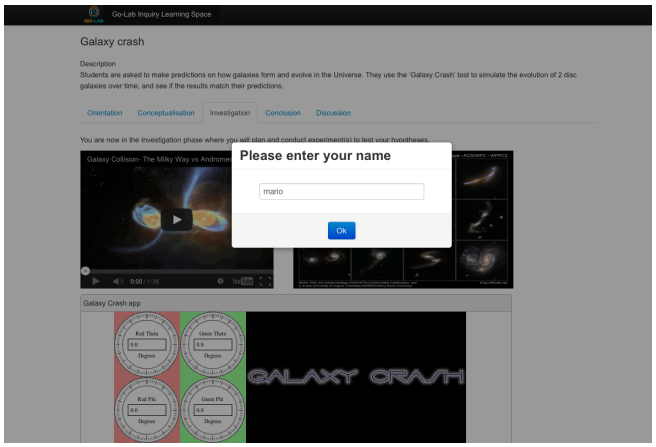

Figure 2: User interface of the *ILS student view*.

Conclusion and future work

In this paper, we analyzed the specific privacy requirements of the Go-Lab portal for students. Based on that, we presented a *classroom-like pseudonymity* approach to protect sensitive student data. The proposed approach follows the privacy paradigm of the real-life classrooms, eliminates the student login and registration burden, and allows personalization. We have implemented a preliminary version of the proposed privacy scheme. In the coming months, the usability of this privacy solution will be evaluated in real classrooms with early adopters.

Acknowledgment

This research is partially funded by the European Union in the context of the Go-Lab project (Grant Agreement no. 317601) under the ICT theme of the 7th Framework Programme for R&D and the PLE Project of the Swiss AAA/SWITCH Program.

References

[1] Bogdanov, E., Limpens, F., Li, N., El Helou, S., Salzmann, C., and Gillet, D. A social media platform in higher education. In *EDUCON*, IEEE (2012), 1–8.

[2] Edelson, D. C., Gordin, D. N., and Pea, R. D. Addressing the challenges of inquiry-based learning through technology and curriculum design. *JLS 8*, 3-4 (1999), 391–450.

[3] Gillet, D., et al. Personalised learning spaces and federated online labs for stem education at school. In *EDUCON*, IEEE (2013), 769–773.

[4] Govaerts, S., et al. Towards an online lab portal for inquiry-based stem learning at school. In *ICWL*. Springer, 2013, 244–253.

[5] Li, N., El Helou, S., and Gillet, D. Using social media for collaborative learning in higher education: a case study. In *ACHI* (2012), 285–290.