6.857 Homework Erica Du Skanda Koppula Jessica Wang	**Problem Set 1**	# 1-1 - An edX Security Policy February 23, 2015

1 Objective

The purpose of this security policy is to outline the security goals and usages of a massive open online course platform (MOOC) like edX. In this document, we define policies regarding user roles and their permissions, as well as privacy and sharing of data.

2 Introduction

EdX is a non-profit, open source MOOC platform that aims to provide educational content to worldwide users. Users sign up on edX and gain access to online courses in a wide range of subjects, administered by accredited universities and organizations around the world. After successful completion of a course, a user may achieve a certificate of completion.

Courses, run by universities, are administered by staff that handle the operations of the course. These staff members control course content and the student experience.

3 Principals and Authorized Behavior

The platform has a hierarchy of user roles. They are, in order: edX employees, universities, course staff, students, and everyone. No user in a role at a certain level has greater permissions than those users in levels above him/her. Each have their own set of allowed functions:

3.1 Course staff

Course staff comprises of both Instructors and TAs. Course staff must be able to perform the following actions:

- Authorize student enrollment into their course
- Authorize other instructors to co-administer their course
- Modify course meta-data (name, description) and content
- Send signed feedback to student

- View the submissions of student enrolled in their course(s)
- Modify their own profile information (email, login username, password)
- Award certificate of completion to select student users.

3.2 Students

When logged in, a student must be able to perform the following actions:

- Request enrollment into a course
- View content for an enrolled courses (to the extent allowed by course instructor(s))
- Submit digitally signed answers and feedback to (enrolled) course instructor
- Modify their own profile information (login username, password, email, payment information)
- Receive certificate of completions as determined by the instructor.

Each student is permitted to recieve only one type of course accredidation after completing the coursework and with course staff approval. Based on whether the student enrolled in the for-credit paid version (Verified Certificate Candidate) or the free version (Honor Code Certificate Candidate), they must recieve the correct certificate, only once.

3.3 edX employees

edX employees manage the platform itself and are able to change any content on the platform. They are limited however, from viewing in plaintext, or modifying any user's personal information, such as passwords, credit card numbers, etc.

3.4 Universities

Administrators and online education coordinators may create accounts on edX to begin authenticating and verifying new instructor accounts at their university. Each university group is verified and approved by edX employee(s). University accounts are able to view and modify instructor and course affiliation with the university. They may also modify their own account details.

3.5 Everyone

Everyone should be able to view an introductory video, read the course description, and read short bios of the instructors of every edX course. Everyone must also be able to register for a new account, or sign in to an existing account.

4 Authentication

- edX password-protects all user accounts. These passwords are encrypted and salted.
- Alternatively, edX also handles authentication through users' Facebook or Google+ accounts.
- Currently the edX platform supports Shibboleth, CAS, and SSL certificates as external authentication sources.

5 Security Goals

5.1 Integrity

Out of the 3 general security goals, integrity is the most relevant and crucial for edX. Since edX-type platforms are metaphorical to a traditional classroom, courses need to maintain the integrity of their data, and unauthorized users such as students or administrators of other courses should not be able to modify a specific course's data. Specific security goals that fall under integrity include the following.

- Ensuring that anyone with permissions of or lower than that of a student cannot change another student's data or course data.
- Ensuring that course staff cannot change data of courses they are not administrators of.
- Ensuring that students cannot change their own data in an abnormal way, e.g. unauthorized modification of test scores.
- Ensuring that students earn completion certificates honorably.

5.2 Confidentiality

Confidentiality is another important goal - the information of edX users should not be compromised to unauthorized parties. In addition, like many online platforms and sites, edX contains sensitive user data such as credit card/billing information and personal details. The main confidentiality goals are the following.

- A student should only be able to see his/her own grades and course content relevant to him/her.
- Course staff should only be able to see their own courses' content and course-related student data.
- A user should only be able to see his/her own sensitive personal/account information such as credit card information.

5.3 Availability

While availability is always important, it has lower priority than other security goals in the context of platforms like edX. Educational courses are not as crucial to its users as other services are to its users, such as hospital systems, space communication systems, and even email. The main availability goal is for all platform data and permissions to be maintained in the event of service unavailability.