Evaluation on Security and Privacy of Web-Based Learning Systems

Yuen-Yan Chan, Chi-Hong Leung and Joseph K. Liu
The Chinese University of Hong Kong,
Hong Kong SAR, China
{rosannachan, leungch}@cuhk.edu.hk, ksliu9@ie.cuhk.edu.hk

Abstract
Web-based learning systems are becoming popular in the recent years. Many courses and lectures are now conducted online. Similar to other web-based applications, security and privacy of Web-based learning systems should not be overlooked. In this paper, we evaluate the security and privacy of general web-based learning systems. We address the security and privacy requirements specific to them. Recommendations on design and implementation of a secure web-based learning system are also presented. In particular, we have evaluated the security services of two popular web-based learning tools.

1. Introduction
Internet technologies change our living habits dramatically. Many daily activities, which once required face-to-face interaction, can now be conducted over the World Wide Web. While security and privacy are important issues in many other web-based applications, however, little consideration of them has been taken into account in the design and implementation of web-based learning systems. In this paper, we analyze the security and privacy requirements of web-based learning systems and address the possible security and privacy threats to them. We will also evaluate the security of two popular web-based learning systems, namely the WebCT [1] and Blackboard [2] systems.

Figure 1 illustrates a three-tier thin client architecture, which is a typical system architecture of state-of-the-art web-based learning systems.

2. Security and privacy requirements and solutions
The five basic security requirements of a system include: authentication, access control, confidentiality, integrity and non-repudiation [3]. Besides, privacy of system users should also be accomplished. For example, user specific information, such as student profiles, learning habit as well as examination performance must not be disclosed to unauthorized parties [4]. During the assessment process, anonymity of candidates should also be provided. That is, the identity of a candidate should be masked from the grader during the marking process so as to prevent bias in the assessment.

2.1. Security threats to web-based learning systems
Security threats present in traditional learning environment, for example, the examination questions, if not physically secure may be exposed to the students prior to the examination. Security threats become more severe when the learning venue is migrated to the networked environment, these threats include:
- Weak passwords can be easily broken.
- In a shared, networked computing environment (for instance, the computers inside a student computer lab), hackers can masquerade the original user by copying the session cookie from a networked computer within the same domain.
- During a web-based examination, students may be able to determine the answers to Javascript-based questions by viewing the HTML page source [5].
- Students can ask third parties to perform the examination or download course materials for them by giving out their logon credentials.
- Anonymity is not provided in most web-based examination and student's identity is revealed to the graders.
- Other general security threats that exist in general web-based systems [6].

2.2. Protection mechanisms

Figure 1. Three-tier System Architecture
Possible protection mechanisms include:
- Use of SSL encryption to provide confidentiality of data transmission.
- Implementation of strong authentication mechanisms.
- Disallowing concurrent logon to prevent cheating in the examination. Alternatively, temporary accounts and passwords, which will only be distributed to students during examination, can be employed.
- Avoid using client-side scripting languages.
- Masking student's identity from grader for the sake of fare assessment.

3. Evaluation of popular web-based learning systems

3.1. WebCT
Security and Privacy features of WebCT are summarized below:
- Authentication: Supports both proprietary ticket-based authentication and browser-based authentication. Single sign-on is supported.
- Access control: Achieved by role-based authorization.
- Confidentiality: Selected data is SSL-encrypted.
- Integrity: Digital signature is not supported.
- Non-repudiation: Relies on activity logs.
- Privacy: Students' performance and course web page usage is not anonymous. Students have no way to control their own information. Moreover, users (include teachers and students) cannot change their own profiles from the WebCT user interface.

A security loophole exists in WebCT in which concurrent logon is allowed. In this situation, a student is able to cheat during examination by passing his/her own user ID and password to an outside party, who then can able to access the same examination paper and submit the paper for the cheater. Such situation can be prevented by additional authentication measures such as using the user's IP address as an additional credential. Also, protection measure as suggested in section 2.2 can also be employed.

4.2. Blackboard
Security and Privacy features of Blackboard are summarized below:
- Authentication: Supports only password-based authentication. Cookies are used so that a user needs not to login once he/she has logged in on the same browser. This authentication mechanism is not secure when the computer is being shared with the others.
- Access Control: Achieved by role-based authorization [7].
- Confidentiality: Supports secure encrypted sessions, including the Secure Shell protocol.
- Integrity: Digital signature is not supported.
- Non-repudiation: Relies on activity logs.
- Privacy: Users can define their own privacy settings and have control over personal information disclosure. However, anonymity is not provided in assessment processes.

By default, Blackboard supports only password-based authentication. In order to provide a stronger protection mechanism, more advanced authentication services such as smartcard-based authentication should be implemented. Also, cookies are employed to provide a more convenient logon process to the users; however, in the campus environment where computers are shared among students, this feature creates a security flaw and it should therefore be disabled. Furthermore, concurrent logon is allowed in Blackboard. Therefore the security loophole discussed in Section 3.1 also exists in Blackboard.

4. Conclusion
In this paper, we have addressed the importance of security of user privacy of web-based learning systems. We begin with the security and privacy issues, as well as their suggested solutions. We have also evaluated the security and privacy services of two popular web-based learning systems, namely WebCT and Blackboard and have pointed out the security flaws in these systems. Corresponding improvement measures are also given.

References