1 Common Criteria

You are developing a Learning Management System (LMS) (e.g., Blackboard or Piazza) that is to be evaluated using Common Criteria. One part of this is a course evaluation *module; the hope is that making this part of the LMS will give higher response rates than the current evaluations. This evaluation should be completely anonymous: the instructor should not even be able to determine if an evaluation comment comes from the same student as a previous anonymous post. However, only students should be able to submit course evaluations, and each student should be able to submit only one.*

Will this require authentication? Develop a Common Criteria functional requirement (selection of options) from Section 12.4 that captures what you think are appropriate authentication requirements for this system. Note that you should do this even if you say this does not require authentication - Section 12.4 includes options of stating explicitly that for some operations, no authentication is required.

FIA_UAU.1.1 The TSF shall allow **entry of items on the course evaluation, but not submission** on behalf of the user to be performed before the user is authenticated.

FIA_UAU.1.2 The TSF shall require each user to be successfully authenticated before allowing any other TSF-mediated actions on behalf of that user.

FIA_UAU.3.1 The TSF shall prevent use of authentication data that has been forged by any user of the TSF.

FIA_UAU.4.1 The TSF shall prevent reuse of authentication data related to authentication for submission of course evaluations.

The above set is a possibility - in this case, the idea is that you get a "token" that allows you to submit once, to enable anonymity without allowing multiple submissions from the same person.

Show how you can use Common Criteria functional requirements to capture the requirement that a course evaluation cannot be traced to any other action of the submitting user.

FPR_ANO.2.1 The TSF shall ensure that **instructors** are unable to determine the real user name bound to **course evaluations**.

FPR_ANO.2.2 The TSF shall provide **course evaluation submission** to **students** without soliciting any reference to the real user name.

Can these requirements apply to everything in the LMS, or do they only apply to the course evaluation? Explain briefly, perhaps giving an example of how these do or don't apply to other parts of an LMS.

Assignment submission, for example, should require a higher degree of authentication (such as non-copiable), and probably should not be single-use. Many parts should not be anonymous, such as assignment submission and providing grades to the registrar. Although perhaps scoring assignments and determining grades should be.

2 Formal Evaluation

The Harrison-Rizo-Ullman access control matrix model can be used for formal evaluation. In particular, Question 10 on the second midterm captures a portion of a formal evaluation of a system satisfying the Bell-LaPadula model. Explain briefly (1-2 paragraphs) what would need to be done to extend the solution to Question 10 to a formal evaluation.

Question 10 (if answered correctly) provides the operations, and the goal that operations should not enable a subject to gain read on a higher-level object or write on a lower-level object. What is needed is a proof that this cannot happen - given any sequence of execution of the commands, the goal will still be met.

I can see an inductive proof - given any initial matrix satisfying the goal, after executing any operation the matrix still meets the goal. Also proving that the level cannot be changed (pretty easy, nothing in the programs writes to those levels of the matrix.) But I didn't expect you to do such a proof.

3 Legal security requirements

We discussed what constitutes a breach under Indiana's Breach Disclosure Law. While this talks about what must be protected, it doesn't say how data must be protected. Identify two sections in the Indiana breach disclosure law that discuss security requirements on ***how*** *data must be protected. For each, give the section number (e.g., IC 24-4.9-2-10(a)(2)), and a one sentence description of why you think this section discusses how data must be protected.*

IC 24-4.9-3-1(a)(2) notes that a breach of encrypted data only needs to be disclosed if the unauthorized person acquiring that data has access to the encryption key. **IC 24-4.9-2-5** defines encrypted data, giving an example of how data can be protected.

IC 24-4.9-2-10 provides that information is not considered "personal information" if it is redacted, **IC 24-4.9-2-11 Redacted data or personal information** says how data can be redacted, a second example.

There are other good answers, but some require digging quite a bit deeper.