Towards Security Requirements in Online Summative Assessments

Kikelomo Maria Apampa, Gary Wills, David Argles
School of Electronics and Computer Science, University of Southampton, UK
{kma07r, gbw, da}@ecs.soton.ac.uk

Abstract: Confidentiality, integrity and availability (C-I-A) are the security requirements fundamental to any computer system. Similarly, the hardware, software and data are important critical assets. These two components of a computer security framework are entwined; such that a compromise in the C-I-A requirements may lead to a compromise of the critical assets. The C-I-A requirements and the critical assets of a computer system are well researched areas; however they may be insufficient to define the needs of a summative e-assessment system. In this paper, we do not discard the existing components; rather we propose security requirements and related components that are specific to summative e-assessment systems.

1 Introduction

Assessment is one of the key activities in student learning. Influenced by technological advances, assessment has begun to make its way out of the traditional classroom into online environments. Thus, employing online assessments delivers benefits such as opportunities for lifelong learning, on-demand learning, automatic marking and immediate feedback. Online formative assessments are designed to improve students' learning and give information about their progress (Rosbottom, 1997).Online summative assessment is categorised as high-stake examinations which takes place at the end of a course of study (Rovai, 2000). In higher education, security considerations do not feature prominently; however this changes when an online assessment is considered (Furnell, 1998). For online formative assessment, issues relating to security are less important as the priority is for students to expand knowledge (Challis, 2005). However, online summative assessments are perceived to be plagued with security challenges which militate against its effective implementation. In this paper, we focus on defining specific security requirements and security attacks in online summative assessments.

2 Existing System Critical Assets, Security Requirements and Threats

Security is a fundamental concept which is relevant in our daily lives and a top priority in several applications. Computer systems require specific security requirements which are fundamental to any system. In literature, the three basic requirements are confidentiality, integrity, and availability (Stallings, 2000; Gollman, 2006). A security relationship exists between the C-I-A requirements and the critical assets (hardware, software and data) of these systems (Pfleeger & Pfleeger, 2003). For example, we assume information data (critical asset) in a computer system. Thus, the data is expected

a. To be accessed by only authorised parties; thus, data must be restricted (confidentiality requirement).
b. To contain no alterations of the original data; modification should be done by authorised parties only (integrity requirement).
c. To be operational and accessible whenever it is needed; except during authorised downtimes (availability requirement).

From the above example, we observe that, the C-I-A security requirements may be employed for summative e-assessment data, such as item bank and assessment data. In a similar approach, the operations of the C-I-A requirements may be applicable to the hardware and software needs of a summative e-assessment system. Examples may include the assessment engine and authoring tools. A security threat launched at the security requirements may cause potential harm to the critical assets of a system. If the security threats are not evaluated and understood; these threats may compromise the confidentiality, integrity and availability of the critical assets (Sandhu, 2002). Thus, existing security threats may be categorised into three broad classes and they describe the forms of attacks launched on a computer system (Stallings, 2000). This threats include interception (attack on confidentiality), interruption (attack on availability), and modification (attack on integrity).

In this paper, we propose that the critical assets of a summative e-assessment system go beyond the hardware, software and data needs; similarly, the security requirements and security threats. However, we do not discard the operations of the existing security components; rather we define security components which are specific to summative e-assessment systems.

3 Electronic Assessment Security

According to Marais *et al* (2006) there are two categories of security in e-assessments: web security and e-assessment security. However, they conclude that web security is a well investigated area but it is insufficient to fulfil the security needs of e-assessment. Generally, during an assessment, it is expected that a potential learner will be present for a test, identified correctly, authenticated genuinely, write a test (delivered through the system), and submit answers to the test. Thus, we propose that the *learner* taking a test is a valuable (critical) asset of a summative e-assessment system. It may be irrelevant for an assessment system to deliver a test with no entity to take the test. In existing computer systems, if a critical asset is compromised; it is perceived that the system has failed to satisfy all of its requirements. Thus, we conclude that the summative e-assessment system will be required to define security requirements which will be suitable for the learner (valuable asset).

3.1 Defining E-assessment Security Requirements

The learner is proposed as a valuable asset to the summative e-assessment system; because if there is no entity at the assessment site taking the test, then the system is perceived idle. Thus, during a summative e-assessment, there are specific requirements which the system expects from a learner. Generally, it is expected that (1) a learner should be present for an online test. (2) a learner should be identified correctly (3) a learner should be authenticated genuinely and (4) a learner should write a test and submit answers to the test. We propose four security requirements expected of the leaner in a summative e-assessment system: presence, identity, authenticity and electronic integrity. In the context of this paper, the proposed security requirements are defined.

a. Presence: requires the physical and online existence of a learner from the beginning to the end of an assessment. Only authorised learners are required to be present continually for the duration of the test.
b. Identity: requires that the learner produce a unique characteristic which distinguishes the learner from duplicates or misrepresentation.
c. Authenticity: requires that the learner provides a proof/evidence/confirmation of genuineness. Only the proof of a learner's uniqueness is required and not a counterfeit.
d. Electronic integrity: requires the single submission of a learner's answers to an online test.

3.2 Defining E-assessment Security Threats

A security threat launched at the security requirements may cause potential harm to the critical assets of a system. Thus, security threats may compromise the security requirements of the critical assets. In electronic assessment security, the security threats which compromise the security requirements are divided into four classes. They include

a. **Impersonation:** this occurs when an unauthorised entity gains access to a system by deceitfully representing a learner at the start, midway or for the duration of an assessment. Examples include illegally writing a test, unlawful external appearances. Impersonation is an attack on presence.
b. **Duplication:** this occurs when an unauthorised entity gains access to a system by misrepresenting the uniqueness of a learner. Examples include illegal use of a learner's identity. Duplication is an attack on identity.
c. **Fabrication:** this occurs when an unauthorised entity creates counterfeit information to prove a learner's uniqueness. Examples include injection of false details into the system. Fabrication is an attack on authenticity.
d. **Corruption:** this occurs when an authorised learner performs fraudulent actions on the system. Examples include doubles submission of test answers. Corruption is an attack on electronic integrity.

4 Analysis of E-assessment Security Requirements

We propose that, presence (P), identity (I), authenticity (A) and electronic integrity (E) are the security requirements in a summative e-assessment system with respect to the learner (asset). However, in this paper, we assume that minimising the security threats affecting the P – I – A requirements may simultaneously minimise the security threats of the electronic integrity requirement. Thus, in this paper the presence, identity and authenticity requirements will be considered. Related work exists based on the electronic integrity security threats and measures (Marais *et al,* 2006; Apampa *et al,* 2008).

In figure 1, the presence requirement poses the question 'are you there?' the identity requirement asks the question 'who are you?' and the authenticity requirement poses the question 'is it really you?' To describe the importance of the three requirements, we consider examples of online systems which employ only two of the three requirements.

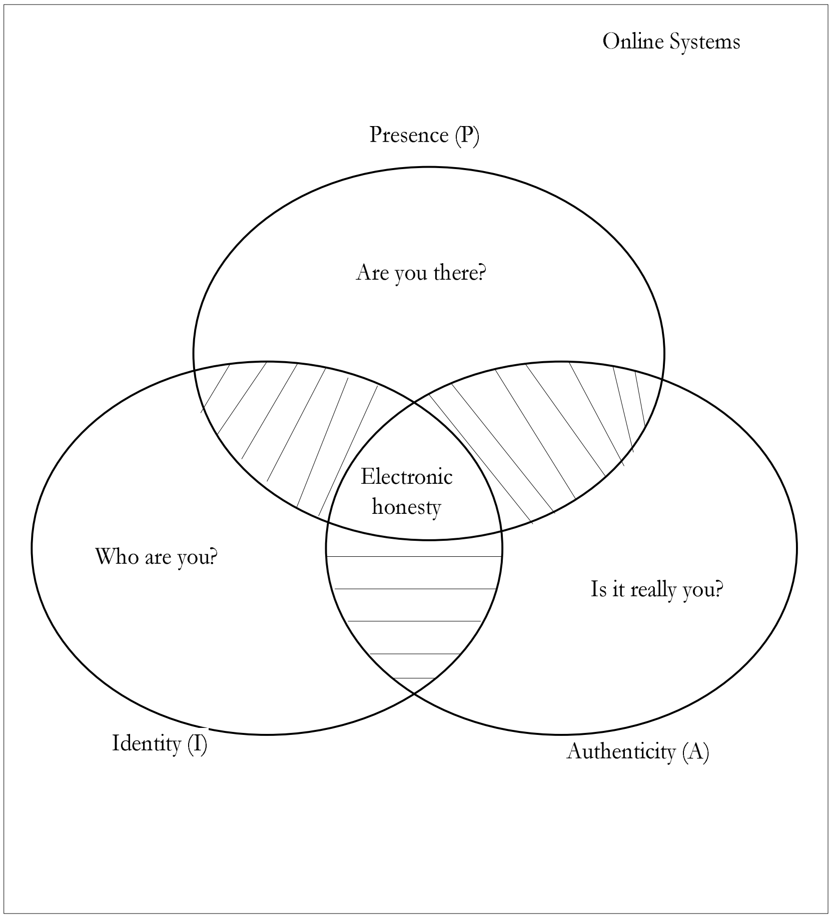

Figure 1 E-assessment security requirements

4.1 Presence and Identity Requirements only

In this system, the entity's presence is of high importance and it excludes the need to prove that the identity belongs to the correct entity. In figure 2, the entity is required to produce a form of identity and be continually present at the location. Thus, these requirements may be suitable for online formative systems. For example, we assume that Alice decides to take an online practice test. She logs on to the website (virtual presence) and she is required to enter a username or email address for identification. The identity is required, such that the system can match a test to Alice for the duration of the test. This may be useful for personalised feedback or marks. Another useful system where the presence and identity requirements may be suitable is in an online gaming system. In most multiplayer games, prospective players are required to log on to the gaming website and adopt nick names for the duration of the game. However, this system may be unsuitable for high-stake summative assessment; because it encourages misrepresentation of identity.

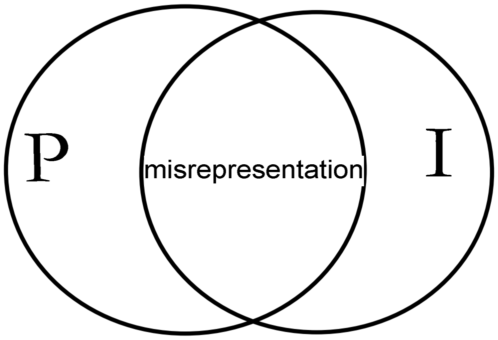

Figure 2 Presence and Identity requirements

4.2 Presence and Authenticity Requirements only

In this system, a proof is required to authenticate presence continually and it excludes the need for an entity to provide an identity. Based on literature survey, the authors of this paper are yet to find a system which relies on presence and authenticity requirements only. Thus, we assume the sets do not intersect (figure 3). However, if such a system exists it may also be fallible to impersonation challenges. As an example, we assume that Alice and Eva are two friends enrolled in a system which requires presence and authenticity only. Irrespective of Alice's method of proof, she may exchange her details with Eva. Therefore, Eva is required to virtually 'show up' and prove her presence by using Alice's proof.

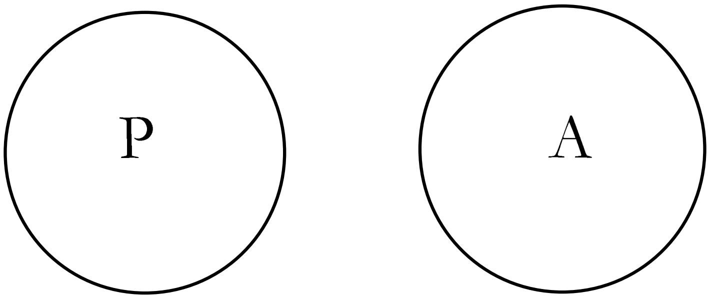

Figure 3 Presence and Authenticity requirements

4.3 Identity and Authenticity Requirements only

In this system, a proof is required to confirm the identity presented by an entity. Irrespective of technologies, the primary aim of these systems is to provide evidence for the identity of an entity. The identity and authenticity requirements (see figure 4) are widely adopted in many online systems including existing online summative environments (1). However, systems adopting the identity and authenticity requirements (excluding the presence requirement) may be highly susceptible to impersonation challenges. In traditional tests, learners are usually expected to possess a learner number as a form of identity and a photo card to authenticate the identity. Using a similar approach, in online assessments learners are issued a username for identification and a password to authenticate the username. However, the technology is gradually fading due to impersonation challenges. In the light of this flaw, biometric technology has been suggested has a unique method for identity or authenticity.

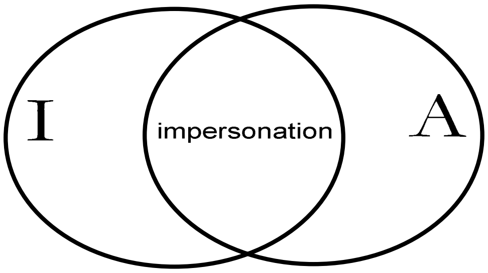

Figure 4 Identity and Authenticity requirements

5 Implications of Employing Two Requirements

From the intersections above, it is noticed that systems which employ only two requirements in their security framework are susceptible to impersonation or misrepresentation threats i.e. $\{P \cap I, P \cap A, I \cap A\}$. In addition, the existing summative e-assessment systems fall into the category of systems that require only Identity and Authenticity $\{I \cap A\}$ requirements. Recall that, impersonation is an attack on the presence requirement. Thus, it is assumed that the exclusion of presence verification in the existing summative e-assessments may increase impersonation challenges in the system. In an existing summative security framework, a learner is required to be identified and authenticated before writing a test. Thus, it is unlikely that the system will continuously verify the learners' presence for the duration of the test. To explain this situation, we assume two scenarios.

Scenarios:

a. Alice and Eva are friends. Alice is present at the assessment site, correctly identified and authenticated to write a test. However, mid-way through the test she employs Eva to complete the test on her behalf. Thus, the system assumes that Alice's details are still linked to the presence represented.
b. Alice and Eva are identical twins. Alice is absent at the assessment site; but employs her twin sister, Eva to write a test on her behalf. Thus, the system is oblivious to the incorrect presence linked to the correct details represented.

We observe that checking only the identity and authenticity requirements may be insufficient to write an online summative test. However, if the presence requirement of a learner is verified continuously; then it is unlikely that the identity and authenticity requirements of the learner will change for the duration of the test. It is noted here, that a continuous verification of the learners' presence does not imply a continuous interruption of the learners' presence. Ideally, the system should not interrupt a learner's test to verify continuous presence; but it is important that presence is checked in a non-intrusive approach.

6 Conclusion

In this paper, we have defined the security requirements that are specific to online summative assessments. We observe that the existing confidentiality, integrity and availability (C-I-A) requirements may be insufficient to fulfil the needs of an e-assessment system. Thus, we propose that presence (P), identity (I) and authenticity (A) are the security requirements expected of a learner (critical asset) in a summative e-assessment system. If a critical asset is compromised; then it is perceived that the system as failed to satisfy all of its requirements. Hence, it is important that a learner is present, correctly identified and authenticated for the duration of an assessment. In addition, we observe that the existing online summative assessment system may be susceptible to impersonation threats (attack on presence requirement); due to employing two requirements i.e. identity and authenticity requirements only. Thus, we suggest that the exclusion of presence verification in summative e-assessments may increase impersonation threats in the system. Our current work focuses on developing a formal model of an online summative assessment system which will show the behaviour of the system when the presence of the learner is verified.

References

Apampa, K. M., G. B. Wills, et al. (2008). Electronic integrity issues in e-assessment security. ICALT 2008: The 8th IEEE International Conference on Advanced Learning. Spain.

Challis, D. (2005). "Committing to quality learning through adaptive online assessment." Assessment in Education 30(5): 519-527.

Furnell, S., P. Onions, U. Bleimann, M. Knahl, H. Rder, P. Sanders. (1998). "A security framework for online distance learning and training." Internet Research 8(3): 236-242

Gollman, D. (2006). Computer Security. West Sussex, England, John Wiley & Sons, Ltd.

Marais, E., D. Argles, et al. (2006). Security Issues Specific to e-Assessments. 8th Annual Conference on WWW Applications, 6-8th Bloemfontein

Pfleeger, C. P. and S. L. Pfleeger (2003). Security in Computing. Upper Saddle River, New Jersey, Prentice Hall.

Rosbottom, J. (1997). Computer managed, open question, open book assessment. Proceedings of the 2nd conference on Integrating technology into computer science education, Uppsala, Sweden., ACM.

Rovai, A. P. (2000). "Online and traditional assessments: what is the difference?" The Internet and Higher Education 3(3): 141-151.

Stallings, W. (2000). Data and Computer Communications. Upper Saddle River, New Jersey, Prentice Hall.