Towards Security Goals in Summative E-Assessment Security

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

The general security goals of a computer system are known to include confidentiality, integrity and availability (C-I-A) which prevent critical assets from potential threats. The C-I-A security goals are well researched areas; however they may be insufficient to address all the needs of the summative e-assessment. In this paper, we do not discard the fundamental C-I-A security goals; rather we define security goals which are specific to summative e-assessment security.

1. Introduction

Online summative assessment is a powerful tool which embodies great benefits such as automated marking, immediate feedback and on-demand tests. Online summative assessments are categorised as high-stake examinations which count towards a final course mark. In higher education, summative e-assessments can be divided into two: (1) e-assessments in supervised environments and (2) e-assessments in non-supervised environments. Summative e-assessments which are conducted in supervised environments include campus based exams and authorised test centres [18]. In these environments, authorised personnel or proctors' are required to monitor and supervise the examination process from start to finish. Non-supervised environments include distance learning examinations and on-demand tests. In these environments, the examination process may be supervised remotely; however the examinee is required to maintain academic honesty. In this paper, we focus on summative e-assessments conducted in supervised/controlled conditions and do not assume a non-supervised environment.

According to Furnell [3], education is not a sector in which security considerations feature; however this changes when an online assessment is considered. Thus, for the purpose of conducting secured summative e-assessment, it is important to define specific security components such as requirements, assets, threats, models, frameworks and goals. In their work, Marais [11] identify two categories of security in e-assessments: web security and e-assessment security. However, they concluded that web security is a well investigated area but it is insufficient to fulfil the security needs of e-assessment. In addition to the well defined web security areas, we include that data security [8] and the network security [18] of summative e-assessments are also well researched. However, we suggest that the user security phase of the e-assessment security is a continuing research field. In this paper, our aim is to present the security goals specific to user security in e-assessments.

2. Assets, Threats and Security Goals

In this section, we define the concepts of assets, threats and security goals in accordance with definitions from security engineering.

2.1. Definitions

An *asset* refers to a resource that might have value, which may be either tangible or intangible that needs to be protected from harm [9]. Types of asset controlled by a system include money, information and data. Identifying the relevant assets of a system can prevent harm to the assets if the system is misused [12]. A *threat* is the potential for misuse or abuse of an asset that will cause harm in the context of the system [7]. The level of harm that can occur depends on the asset type. Therefore, it is appropriate to identify the relevant threats that may apply to each asset type. A *goal* is something people interpret differently depending on the nature of job they are doing. For example, a goal would mean differently to a footballer, psychologist or an engineer. In general, a goal expresses what is desired. It can also refer to a specific, measureable occurrence that any business or system plans or intends to achieve or avoid. One method of generating the *security goals* of a system is by specifying that the actions on the assets listed in threat descriptions can be prevented [8].

2.2. Confidentiality, Integrity and Availability

The hardware, software and data of computer systems are widely recognised as valuable assets [15]. In computer network systems, the network medium is also regarded as a critical asset. The security goals which ensure that the hardware, software and data assets are not compromised include confidentiality (C), integrity (I) and availability (A) [5]. In literature, it is suggested that a security relationship exists between the C-I-A security goals and the critical assets (hardware, software and data) of a system [15]. Thus, a compromise in the C-I-A security goals may lead to a compromise of the critical assets. To explain the existing security relationship, we present an example of data stored in a computer. The data is expected:

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

As described in [13], the threat of unauthorised exposure is converted to the goal of protection from unauthorised exposure, commonly known as confidentiality. Similarly, the threat of unauthorised alteration is converted to the goal of integrity. Using a similar approach, the C-I-A security goals can be applied to summative e-assessment data (e.g. items stored in the item bank) to prevent data from potential threats. In addition, the C-I-A security goals may be applied to protect the hardware (server) and software (application) needs of a summative e-assessment system.

3. E-assessment Assets, Threats and Security Goals

In this paper, we propose that the valuable assets of a summative e-assessment system extend beyond the hardware, software and data needs. It should be noted that, we do not discard the importance of the above assets; rather we present assets which are specific to the e-assessment system. Online summative assessments are regarded as tests which are taken to produce a feedback of teaching and learning. A lecturer sets a test based on his/her course materials, and the student is required to answer the questions. Since summative assessments count towards a student final mark; then a student will do all to pass. Based on the definition of an asset (see section 2.1), we propose that a student taking a test is a valuable asset to the summative e-assessment system. In addition, an online assessment system is perceived busy, when it is providing an online test for a student.

A security threat launched on a system may cause potential harm to the critical assets. Security threats may be a deliberate or non-deliberate act [19]. Thus, we describe three types of possible harm which a student (asset) may deliberately put in effect:

- *T1:* Incorrect and illegal student taking a test
- *T2:* Falsification of identity detail
- *T3:* Abuse of authenticity detail

Having identified the asset and the potential threats of a summative e-assessment system, we propose that the C-I-A security goals may be unsuitable to prevent the asset from the threats. As depicted in section 2.2, the C-I-A security goals are better suited for assets which are not directly dependent on humans. It is observed that during an online test a student is required to interact with the machine (hardware asset). Thus, the C-I-A security goals can be applied to the machine; however, the student is unable to satisfy the C-I-A security goals independently. Furthermore, it is practically unlikely to determine if a student taking an online test satisfies the C-I-A security goals. Hence, we propose three security goals to be satisfied by the student taking an online assessment. It should be noted that we do not disregard existence of the C-I-A security goals; however we define security goals specific to user security:

- *SG1:* Prevent incorrect and illegal student taking a test. This is described as the goal of **Presence.**
- *SG2:* Prevent falsification of identity detail. This is described as the goal of **Identity.**
- *SG3:* Prevent abuse of authenticity detail. This is described as the goal of **Authentication**.

Table 1. Security goals and related questions

Security Goals	**Security Questions**
Presence	Are you there?
Identity	Who are you?
Authentication	Is it really you?

4. Identity and Authentication Security Goals

The identity and authentication security goals are existing goals needed to fulfil the user security phase of an online assessment. During a summative test, a student is required to provide answers to the “who are you?” and “is it really you?” questions (see table 1). Security research in summative e-assessment has concentrated on developing secure mechanisms to assists students in providing and proving this answers. The username and password technique is a widely acceptable method to confirm student legitimacy. Another method is the use of biometrics, which is suggested as an ultimate identity and authentication technique for e-learning [11]. Irrespective of known biometric challenges [2, 10, 17], researchers explore the possibilities of employing biometrics in e-assessment. Current researches focus on multi-biometrics to support services for identity and authentication [3, 16].

Regardless of the techniques employed, the identity and authentication of a student remains a major challenge to the summative e-assessment process [1, 8]. Hence, we do not suggest the unsuitability of the mechanisms used; rather we propose that satisfying the identity and authentication goals alone is insufficient to ensure user security. It is reminded, that this paper is focused on e-assessments within a supervised environment and not a remote distance learning environment. Thus, the example and scenarios presented relate to the activities in a controlled environment. The example is identified through sources such as interviews with e-assessment officers, personal e-assessment experiences and complimented with literature review to provide a balance. The relevant excerpts are described in the example below.

4.1. Summative E-assessment Example

We assume that, COMP101 is a compulsory undergraduate module in a Computer Science department. During online summative assessments, students are required to enter their identity and authentication details to verify their legitimacy. The student will proceed in the assessment if there is an exact match with the stored details; however, if there is no match the student will retry. During the test, an authenticated student may carry out any (or none) of these actions: (1) need the toilet; thus leaving the exam room, (2) finish the exam early and (3) feel sick. Based on the above example, we describe two scenarios

1. We assume that Alice is registered for the COMP101 course. However, on the exam day Alicia shows up to represent Alice. Alicia enters Alice's username and password to continue with the assessment.
2. We assume that Bob is registered for the COMP101 course. On the exam day, Bob enters his username and password to continue the assessment. During the test, Bob takes a break (e.g. toilet) and exits the assessment lab. However, Bob does not return to continue the test; instead Tom logs into the PC and resumes Bob's test.

The above scenarios depict an e-assessment process, where the students are assumed trusted and the invigilator only monitors the events which occur in the examination room. Scenario 1 describes a typical case of impersonation, where a student willingly shares his/her identity and authentication details. Weippl [22] asserts that students who want to cheat willingly collaborate with the person who tries to impersonate as them. In contrast, people will not knowingly cooperate with someone who tries to steal their money out of their bank account [22]. Therefore, in online summative assessments a student cannot 'accidentally' impersonate another; there must be an exchange of identity and authentication details [21]. In scenario 2, a correctly authenticated student can also be impersonated during the assessment. The impersonator in scenario 2, is only required to posses the identity and authentication details of another student to enable him resume the test. In scenario 1 and scenario 2 it is shown that the only requirement needed to write a test is a student's identity and authentication details. Furthermore, it is unlikely that the machine will spot the difference between a legal and an illegal student; as long as the details required are correct. Hence, satisfying the identity and authentication security goals may not be enough to ensure user security.

5. Presence Security Goal

In this section, we introduce presence as an important security goal of an online summative assessment. To clarify any confusion between the identity and the presence of a student, we define these terms as used in this paper. Identity refers to a distinguishing characteristic of an entity which differentiates the entity from other entities whilst, presence is a natural phenomenon which reflects a state of an entity being at a specific space or place. We discuss two types of presence specific to e-assessment; the physical presence and the electronic presence.

5.1. Physical Presence

In summative e-assessment, the physical presence of a student describes the ability of the student to occupy space in a given location (e.g. exam hall). During an online assessment, an invigilator is required to check the students ID card to verify correct physical presence. Therefore, a photo on the student ID card is manually matched with the face represented. The student will proceed with the assessment if there is a close match between the face and the photo presented. Modifying the example described in section 4.1, we introduce an invigilator to manually verify the students' presence before they can enter their identity and authentication details. This method is useful and it is a common approach to prevent impersonation in summative e-assessments [20, 23]. Based on the modified example, we again describe one scenario

1. We assume that Alice is registered for the COMP101 course. However, on the exam day Alicia shows up to represent Alice. Alicia presents Alice's student ID card and the invigilator confirms that her face matches the photo on the ID.

The above scenario depicts an online assessment process, where an invigilator confirms the students' presence and monitors the events of the examination. In the scenario, it is observed that an incorrect student (Alicia) presents a correct student ID card (Alice) and the incorrect student is allowed to write the test. We suggest two possible events for this occurrence

- An invigilator may be unable to differentiate between lookalike students.
- An invigilator may have connived with the students to enforce the fraudulent act. This is connived impersonation.

It is not uncommon to find lookalike friends, family members or identical twins; such that it is difficult for an invigilator to spot the difference. If this occurs, then the impersonators will proceed to write the e-assessment undetected. The second event is a probability of connived impersonation which has often been overlooked in campus-based assessments. However, it is important to prevent any form of connived impersonation; as the impersonators will surely proceed undetected.

5.2. Electronic Presence

In order to clarify the definitions of electronic and online presence, we firstly describe the concept of online presence. In literature, the term online presence is widely employed when business transactions are conducted via the internet. Thus, these businesses are required to create and maintain a strong online presence, to have an impression on potential customers [14]. Online presence is also prominent during instant messaging and visual representations known as avatars are used to depict online persona. There is a blurry line between the definitions of online and presence and electronic presence. However, we define electronic presence as a state in which a students' physical presence is electronically verified and monitored for the duration of an online assessment. We propose that, combining electronic presence with the identity and authentication security goals will improve the user security of summative e-assessments. Based on the examples described above, we revisit the scenarios

1. We assume that Alice is registered for the COMP101 course. However, on the exam day Alicia shows up to represent Alice. An electronic presence sensor detects Alicia's presence and takes an image. When Alicia enters Alice's identity and authentication details, the system restricts her from proceeding with the assessment.
2. We assume that Bob is registered for the COMP101 course. During the test, Bob takes a break; however, Bob does not return to continue the test. Tom returns to resume Bob's test but the system restricts him from proceeding with the assessment.

In the above scenario, Alicia is unaware that an image of her face is captured and matched against the stored identity and authentication details. Unknown to Alicia, Alice's stored image is tied to her identity and authentication details; thus, Alicia is restricted due to image and details mismatch. Bob could write the assessment, because the image taken initially corresponds to his identity and authentication details. When Tom enters Bob's details, an image is captured and matched to the details typed. Tom is restricted, has the image do not match the information (Bob's image and details) stored for the initial test taker. In an alternative method, a student's electronic presence, identity and authentication details may be tied to a static IP address; which is available only for the student. Furthermore, if electronic presence is verified then the chances of a lookalike family member or friend being successful in impersonating another student will be very low. Similarly, the probability of a connived impersonation will be reduced, as the verification of presence is not dependent on the invigilator.

6. Conclusion and Future work

This paper does not disregard the importance of confidentiality, integrity and availability (C-I-A) security goals in e-assessment; however we define security goals that are specific to summative e-assessments. In this paper, we propose that a student taking an online test is a valuable asset; thus, presence, identity and authentication are security goals which are expected of the student during an e-assessment. It is shown that the existing identity and authentication security goals are susceptible to impersonation threats, if the presence security goal is excluded. We divide the presence security goal into physical presence and electronic presence. However, we show that satisfying the physical presence goal is vulnerable to undetectable lookalike friends and connived impersonation threats. We suggest that, integrating the electronic presence with the existing identity and authentication security goals will improve user security in summative e-assessment systems.

Our current work focuses on developing a formal model of an online summative assessment system which would satisfy the electronic presence security goal. Firstly, we aim to model the behaviour of a system with the identity and authentication (I-A) security goals only. Secondly, we will model the behaviour of a similar system with the electronic presence security goal inclusive (P-I-A). Finally, our goal is to compare the two systems and determine the effect of electronic presence on summative e-assessment security.

7. References

[1] Aojula, H., J. Barber, R. Cullen., J. Andrews. (2006). "Computer-based Online Summative Assessment in Undergraduate Pharmacy Teaching." *Pharmacy Education* **6**(4): 229-236.

[2] Apampa, K. M., Zhang, T., Wills G.B., Argles, D. (2008). “Ensuring Privacy of Biometric Factors in Multifactor Authentication Systems”. SECRYPT 2008: International Conference on Security and Cryptography (ICETE). Portugal.

[3] Asha, S., Chellappan, C**.** (2008). “Authentication of e-learners using multimodal biometric technology” International Symposium on Biometrics and Security Technologies, ISBAST. Islamabad.

[4] 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

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

[6] Haley, C. B., Laney, R. C., Moffett, J.D., Nuseibeh, B. (2008). "Security Requirements Engineering: A Framework for Representation and Analysis," *Transactions on Software Engineering (IEEE)* **34**(1): 133-153

[7] Haley, C. B., Laney, R. C., Nuseibeh, B. (2004). "Deriving Security Requirements from Crosscutting" Software Development (AOSD'04). Lancaster, UK: ACM Press, 22-26 Mar, pp. 112-121.

[8] Hernandez, J.A., Ortiz, A.O., Andaverde, J., Burlak, G. (2008). “Biometrics in Online Assessments: A Study Case in High School Students”. 18th International Conference on Electronics, Communications and Computers. CONIELECOMP, Puebla

[9] ISO/IEC. *Information Technology - Security Techniques - Evaluation Criteria for IT Security - Part 1: Introduction and General Model*, 15408-1. Geneva Switzerland: ISO/IEC, 1 Dec 1999.

[10] Jain, A. K., K. Nandakumar, Nagar, A. (2007). “Biometric Template Security”. *EURASIP Journal on Advances in Signal Processing,* Hindawi Publishing Corporation.

[11] Marais, E., D. Argles, von Solms, S.H (2006). “Security Issues Specific to e-Assessments”. 8th Annual Conference on WWW Applications, Bloemfontein.

[12] Moffett, J. D., Haley, C. B., Nuseibeh, B. (2004). "Core Security Requirements Artefacts," Department of Computing, The Open University, Milton Keynes, UK, Technical Report 2004/23.

[13] Moffett, J. D., Nuseibeh, B. (2003) “A Framework for Security Requirements Engineering”, Department of Computer Science, YCS368. University of York, UK.

[14] Moore, C.W (2008). *Managing Small Business: An* Entrepreneurial *Emphasis, International Edition.* South Western College, Publishing.

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

[16] Rabuzin, K., Baca, M., Sajko, M. (2006). “E-learning: Biometrics as a Security Factor” International Multi-Conference on Computing in the Global Information Technology, 2006. ICCGI. Bucharest.

[17] Ratha, N. K., S. Chikkerur, Connell, J.H, Bolle, R.M. (2007). "Generating Cancelable Fingerprint Templates." *IEEE Transactions on Pattern Analysis and Machine Intelligence* **29**(4): 561-572

[18] Rowe, N. C. (2004). "Cheating in Online Student Assessment: Beyond Plagiarism." *Online Journal of Distance Learning Administration* **VII** (II).

[19] Sandhu, R. S., P. Samarati (1994). Access Control: Principles and Practice. IEEE Communications Magazine. **32:** 40-48

[20] Stoner, G. (1996) “Implementing Learning Technology” Learning Technology Dissemination Initiative. Heriot-Watt University, Edinburgh

[21]Vollans, T. (2008) “The Law School with two Masters?” *Web Journal of Current Legal Issues* http://webjcli.ncl.ac.uk/2008/issue2/vollans2.html (accessed 10 July, 2009)

[22] Weippl, E. R. (2005). *In-depth tutorials: Security in e-learning*. eLearn Magazine.

[23] Weippl, E. R. (2006). “On the Use of Test Centers in e-Assessment”. *E-Learning Reports*, Vienna University of Technology.