ABSTRACT

Two challenges with online assessment are making sure data collected is secure and authenticating the data source. The first challenge relates to issues such as network security, robustness against attack and data management. The second is currently a significant impediment to widespread implementation of formal online assessment due to difficulties ensuring the identity of the person completing the assessment. In this chapter the authors discuss technical aspects associated with keeping data secure and the implications this has for delivering online assessment. The chapter also examines technologies that can assist with the issue of authenticating the identity of individuals completing online assessments and we provide some practical advice for those considering using online assessment tools. To conclude the chapter, the authors look at technologies likely to be available in the future and examine how these could be used to conduct online assessment that ensures data security and integrity without imposing an unreasonable burden on users.

INTRODUCTION

While online or e-assessment has many potential benefits for both students and teachers, it is not without its challenges. As with traditional methods for delivering examinations, the procedures associated with online assessment need to ensure any assessment data is secure. This means ensuring exam materials are only accessed by those who are entitled to access them, and that any access
Ensuring Security and Integrity of Data for Online Assessment

is appropriate to the user’s role. The second challenge is authenticating the source of the data and being able to ensure the identity of the person completing the assessment. In this chapter, we are concerned with issues relating to security and integrity of assessment data transmitted online over any network - fixed or mobile, wired or wireless. We examine the four key functions technology can facilitate and discuss their application in the context of online assessment. Examples from the first author’s experience teaching and assessing online are used to illustrate the practical implications for staff wanting to use online assessment. We also briefly look at future technologies and how they could fundamentally change how we do online assessment.

BACKGROUND

Conversations about online assessment generally reveal two schools of thought. Supporters will often talk about the flexibility online assessment provides such that students are able to take a test anywhere and at any time (Cann, 2005; Engelbrecht & Harding, 2004). Or they mention the decreased administrative and marking overheads associated with online assessment as a significant benefit (James, McInnis, & Devlin, 2002; Nicol, 2007a). Online assessment tasks can also assist educators to assess a broader range of skills, provide students with different types of assessments, including ones not easily achieved using traditional assessments methods. They can also provide students with benefits such as timely and informative feedback on their progress, as well as teaching students new skills and ways of studying and learning (James, et al., 2002). The second group most frequently point to the difficulties associated with verifying the identity of the person taking an online test, or they express concerns about how to stop cheating and the problem with networks crashing during tests. They might also be understandably concerned with protecting the confidentiality of assessment material, wanting to be sure that assessment material is not accessed by unauthorized persons, that assessment data, including student responses and grades, are not altered. What is often missing in these vigorous and important discussions is an understanding of how technology can be used to address some of the very valid concerns associated with online assessment and what additional benefits it can provide if implemented appropriately.

Dependability is the key requirement for e-assessment according to Weippl (2007), which encompasses a number of factors including availability, reliability, safety, integrity, and maintainability. He stresses that when e-assessment is used for examinations, all these aspects of dependability become critical. The assessment needs to be available when it is required, so measures should be in place to prevent attacks on availability, which are referred to as Denial of Service (DoS) attacks. Not only must the service be available when required, but there needs to be continuity of the service. Before, during and after the exam the integrity of exam questions and materials, student responses and grades need to be ensured. Any system used to deliver an online exam needs to be safe and maintainable. The essentials of secured networks include having a proper network security policy, enforcing identification, confidentiality and integrity and implementing proper compliance monitoring mechanisms (von Solms & Marais, 2004).

While aspects of safety and maintainability seem to be mainly a responsibility of the Information Technology (IT) department in higher education institutions for example, as we will see, responsibility for availability, reliability and integrity belongs to those preparing, administering and marking the exam as well as the IT department. Online exams can fail for reasons such as software bugs as well as because of hardware or other infrastructure failure. As Weippl points out, “[E]-learning has a strong technological component but it is important to keep in mind