Chapter 3
Mitigation of Cheating in Online Exams: Strengths and Limitations of Biometric Authentication

Aparna Vegendla
Norwegian University of Science and Technology, Norway

Guttorm Sindre
Norwegian University of Science and Technology, Norway

ABSTRACT

E-exams have different cheating opportunities and mitigations than paper exams, and remote exams also have different cheating risks than on-site exams. It is important to understand these differences in risk and possible mitigations against them. Authenticating the candidate may be a bigger challenge for remote exams, and biometric authentication has emerged as a key solution. This chapter delivers a categorization of different types of high-stakes assessments, different ways of cheating, and what types of cheating are most relevant for what types of assessments. It further presents an analysis of which threats biometric authentication can be effective against and what types of threats biometric authentication is less effective against. Insecure aspects of various biometric authentication approaches also indicate that biometric authentication and surveillance should be combined with other types of approaches (e.g., how questions are asked, timing of the exam) to mitigate cheating.

INTRODUCTION

Cheating is a significant threat against high-stakes university exams (McCabe, Trevino, & Butterfield, 2001), whether the exams are conducted on-campus (Cizek, 1999) or online (Nixon, 2004; Rowe, 2004). Successful cheating may reduce the credibility of universities and their diploma, create unfair advantages for cheaters over the honest, hard-working students, and ultimately be detrimental to the university’s learning culture (Davis, Drinan, & Gallant, 2011).

DOI: 10.4018/978-1-5225-7724-9.ch003
Impersonation (e.g., having somebody else sit a test for you) is not the most frequent way of cheating at university. Sheard et al. (Sheard, Dick, Markham, Macdonald, & Walsh, 2002) in a questionnaire survey of two Australian universities, found that only around 2% of students reported ever having hired a stand-in for an exam, and there were also a few who had hired somebody else to do graded homework assignments for them, while there were much higher percentages for various other types cheating. McCabe (McCabe, 2005), based on surveys with 80,000 North American students, indicated that the most common cheats for examinations were acquiring test questions ahead of time and copying answers among students during the test. For written assignments (e.g., take-home work), the most common cheats were collaboration (or Collusion) and usage of assistance on work supposed to be individual, as well as small fragment plagiarism.

Even if impersonation is not the most common way of cheating, it is important to protect against. Whereas the actual grade gain of some other cheating approaches is often limited, impersonation can boost somebody’s grade all the way from F to A, given a sufficiently competent stand-in. Moreover, impersonation is difficult in a small class context where the staff administering the test knows the students personally, the chance of successful impersonation increases in large class settings, and even more so for distance education with remote exams.

This is further accentuated in online courses due to the availability of technology and internet in exams conducted in un-controlled remote environment (Agulla, Rifón, Alba Castro, & Mateo, 2008). Indeed, in the early days of online exams, distance education there were many arguments that students would have to travel to proctored locations for high-stakes tests, since it was just too easy to cheat if allowed to take the exam at home.

In many application domains faced with a threat of impersonation (e.g., somebody else claiming to be the legitimate user), a typical solution is to combine several factors of authentication for increased security. A factor can be something that the user (i) knows (example: password), (ii) has (example: access card, one-time pin-code generator), or (iii) is, i.e. biometric properties of the user (Firesmith, 2003). All the authentication methods have their own advantages and disadvantages (Idrus, Cherrier, Rosenberger, & Schwartzmann, 2013). As for biometric properties, these can be either Physiological (example: fingerprint, hand geometry, palm print, iris, face, DNA) or behavioral (example: gait, voice, lip movements, handwriting, keystroke dynamics). When authenticating students for an exam, factors of type (i) and (ii) are inherently insecure because potential cheaters may want to be impersonated. Hence, biometrics should be the preferred means of authentication for exam candidates, and if the combination of several factors is found necessary, this should be two different biometrics rather than combining with passwords or tokens. Traditionally, a kind of “manual biometrics” have been used, students having to show picture ID cards. However, this is vulnerable to stand-ins with similar looks, as well as to fake IDs, as for instance illustrated by the news article (Anderson & Applebome, 2011). Computer supported biometric authentication would be clearly preferable, both for increased security and saving manual authentication work by exam proctors. A major problem of biometric authentication is that it is not free from errors in the extraction of the human characteristics and comparison of biometric data. A typical solution is to combine more biometric features using multi biometric authentication which is more reliable compared to single biometric technology or unimodal (Asha & Chellappan, 2008).

The idea of using biometrics for authentication of remote exam takers is not new, there were proposals for this more than a decade ago (Hernández, Ortiz, Andaverde, & Burlak, 2008; Levy & Ramim, 2007; Ramim & Levy, 2007). However, technology for biometric authentication has made much progress recently, offering a wider range of measures to mitigate cheating. At the same time, cheating techniques