Chapter 13
The Issues Related To Student Authentication in Distance Education

Deb Gearhart
Troy University, USA

ABSTRACT
As long as there has been distance education there has been the question, ‘how do you know the student turning in the work is the student registered for the course?’ As technology has been improving distance education course delivery, online education has been growing in leaps and bounds. The most recent Sloan-C report stated that in the U.S. alone there were almost 3.9 million students taking at least one online course during the fall of 2007 term (Allen and Seaman, 2008). Legislators took a hard look at the issue of student authentication in distance education with the passage of the Higher Education Opportunity Act of 2008. This paper reviews the issues related to student authentication and reviews the current forms of student authentication, reviewing one institution’s answer to student authentication in its online programs.

BACKGROUND
To understand the issues related to student authentication a little history on distance education and an understanding of biometrics is needed as background. Distance education in the United States has been around for about 125 years. Educators have been trying to provide educational experiences to meet the needs of underserved students. Starting with the print based medium, know for many years as correspondence study, institutions have met the needs of learners around the country. Other media followed including radio, television, audio and video recordings, audio and video conferencing, computer mediated instruction and with the introduction of the Internet, what is now known at online learning (Wang & Gearhart, 2006).
One of the issues that has been around as long as there has been distance education is the issue that the student registered for the course is the student doing the work, student authentication. Why the concern for student authentication in distance education? Primarily because not all students are ethical and some do cheat. Over the years students have found ways to cheat on assignments and exams. Students have had other students do work for them and turn it in as their own; students have plagiarized papers, students will cheat on exams. Studies have shown that cheating is on the rise. McCabe and Trevino (2002) noted that cheating reported on nine campuses grew from 26% in 1963 to 52% in 1993. Gearhart (2007) discussed an additional replication of the study in 2001 noting that 72.8% of the students reported cheating. Part of the disconnect with cheating involves students’ own perceptions of their own roles in a course. Craig, et. al. (2008) reported in their study that 87% of the students felt it was important to submit their own work, yet the studies on student cheating continue to grow. Students will comment it is important to do their own work, to not cheat, however, especially in the case of online learning, where students do not directly see the consequences of their actions find it does no harm to cheat (Gearhart, 2007).

Distance education administrators have been dealing with the issue of student authentication for many years. One way, which is the emphasis of this paper, is dealing with academic integrity of an online course through the use of a proctored exam. Proctored exams have been a means for academic integrity for many years. Distance education programs have used human proctors and a complex proctor approval process to ensure academic integrity of student coursework. However, finding and approving human proctors is not an easy task. In this day and age of technology integration, use of technology for student authentication has become more prominent. The next few sections of this paper explain the forms of authentication and how they can be used with technology and in higher education to set up the case study of one institution’s resolution to this issue.

AN INTRODUCTION TO BIOMETRICS

Fingerprints are the ridge and valley patterns on the tips of the fingers and are the oldest and most accepted form of biometrics. Ancient kings and queens sealed letters and authenticated them with fingerprints in the wax thousands of years ago. Over hundred years ago, in the US and in Europe fingerprints were used for identification. In all this time, no two fingerprints have been found to be the same. They are truly unique to each individual (Upendra, Singh, Kumar, and Verma, 2007). Upendra, Singh, Kumar, and Verma (2007) explain how online fingerprint systems work. During the registration process a reference biometric template of the fingerprint is stored in a database. Then when the authentication process, when the user is being verified, the biometric template is reviewed and used to match at the established threshold. According to Crews, Jr. (2003) authentication is now commonplace in society with face recognition cameras found in airports, city streets, among other public places. Other forms of biometric authentication have developed. Langenderfer and Linnhoff (2005) describe the biological traits used for authentication purposes including fingerprints, face, palm, hand geometry, hand vein pattern, fingernail bed, iris, retina, body odor, skin reflection, ear shape, teeth, and DNA; while voice, lip motion, signature, gait, and keystroke dynamics have been used as behavioral measures. Many of the technologies are beneficial for security reasons. Crews (2003), however, is concerned about the point at which such technology goes beyond voluntary to becoming an invasion of privacy to the point where a potential loss of fourth amendment protections cab occur. Will we be forced to mandatory biometric identification? These issues