Distance Learning Student Authentication: Verifying the Identity of Online Students

Jeffrey L. Bailie and Michael A. Jortberg

Abstract

This session will address how one university has partnered with a corporation to work in partnership on the verification of online student identity. Through this collaboration, the university seeks to enhance the credibility of its online evaluation process by employing data forensic techniques commonly utilized by today's financial services industry. Bailie and Jortberg will present details on how user authentication strategies are being applied as a means to verify remote learner identity during formal online performance appraisals.

Perhaps more than ever before, today's adaptation of distance education offers an analogous academic alternative to the traditional classroom experience for students who desire a learning opportunity more consistent with their individual lifestyles. Many of the advancements that have allowed for an increasingly convenient system of delivery have materialized as technology continues to influence the landscape of distance education. Increasingly, online course offerings are becoming somewhat of a necessity for universities as they strive to meet the changing interests of a constituent base that demands a wide range of options in academic pursuits. Barriers of time and place that once presented obstacles to enrollment are now overcome through the relative flexibility found in Web-based delivery. Yet while technological advancements of the past decade have shaped a more ubiquitous delivery of online learning, online learner evaluation has not always maintained the stride.

Historically, the assessment of student learning in a distance education environment has not been without challenge. After all, how an institution validates the true identity of the individual actually completing the coursework has been questioned by those critical of distance education. As a result, institutions of higher learning have found it necessary to contemplate various alternatives for the assessment of learner performance at a distance. Among such alternatives are adaptations to the conventional means of "secure" on-ground, face-to-face examination including:

- Increased emphasis on student portfolios, papers, projects, and quizzes in exchange for high "point weighted" midterm and final tests
- Utilization of proctored assessments administered at sanctioned testing centers
- Use of advanced technology intended to validate an individual's biometrics, including fingerprint readers, retinal scanners, and facial or voice recognition programs
- Synchronous monitoring, including video surveillance, telephone call-back, IP or cookie authentication, and software that detects discrepancies in response patterns such as typing speed
- Complete avoidance of secure testing

Even with the available and emerging alternatives, the pressure to find a reliable and cost-effective protocol to securely evaluate students engaged in online programs continues to increase, as evidenced by recent legislation leading to the reauthorization of the Higher Education Act (HEA). Specifically, the College Opportunity and Affordability Act (H.R. 4137), which was passed by the Committee on Education and Labor in the U.S. House of Representatives on November 15, 2007, corresponds with a bill passed by the U.S. Senate (S. 1642) in July 2007. Both pieces of legislation contain verbiage directing accreditation agencies to "require an institution that offers distance education to have processes through which the institution establishes that the student who registers in a distance education course or program is the same student who participates in and completes the program and receives the academic credit." (H.R. 4137, 110th Congress, 2007). Accordingly, if the most recent versions of the of the bill progress, proving an individual's identity in the interest of maintaining online program integrity will undoubtedly become a new requirement to be included in the process of accreditation.

National American University (NAU), in collaboration with Acxiom Corporation, has successfully piloted a program for the verification of students enrolled in the university's online courses. The basis of the pilot program incorporates the use of personal data collected outside the university, as provided and managed by a independent corporation that specializes in forensic consumer data services more commonly associated with the financial industry.

Features of Online User Verification

The development of a user verification strategy begins with an appreciation for the interrelated components necessary to construct a well-designed system, as well as the function each component offers in establishing the broader system. The basic strategy for the management of a secure system of user access is based on four crucial features: identification, authentication, authorization, and accountability (IAAA).

Identification relates to the initial establishment of an individual's factual identity. In its truest sense, this is an assurance that an individual presenting himself as Bill Jones actually is Bill Jones. For students, this is a standard undertaking at the time they apply for admission prior to formal enrollment. Identification activities begin with the collection of personal information used as further proof of identity, including facets such as legal name and address, social security number, academic records, and so on. Subsequent to formal enrollment, online students are issued a token (such as a user name) to be used as an identifier to access a secured online course.

Authentication relates to the validation that the entity offering the identification token is actually the one assigned to use it. This feature involves the authentication of a key identification factor that should be unique to the user. The technology available for fraud mitigation relies on four main premises of identity authentication:

1. Who we are—fingerprints, iris scans, voice recognition, DNA, and so on
2. What we have—birth certificate, driver's license, passport, digital tokens, and so on
3. What we know—in-wallet and out-of-wallet information about our past, such as financial, geographical, and demographic data
4. Where we are at a specific moment in time—video monitoring, IP address, telephone access, and so on

Authorization is the certainty that the entity is granted access only to areas where he/she has been bestowed proper privilege or authority. This feature offers an assurance that access is restricted only to approved areas, functions, or tasks. For online learners, this would suggest that once accessed, only select elements of the course would be made available.

Accountability is the assurance that only authorized entities have accessed the secure system. This is the ultimate element of credibility that is being sought in an online testing environment. Accountability is achieved when proper identification, authentication, and authorization has been accomplished (Bruhn, Gettes, and West 2003).

The NAU-Acxiom Pilot Project

As with many other distance education programs, NAU's virtual campus has evolved in response to increasing enrollment and the expanding range of services necessary to effectively provide for students, regardless of time and place. Since 1996, NAU has assembled a delivery infrastructure designed to ensure a dependable learning experience. During this time, the university investigated cost-effective alternatives for the assessment of learner performance at a distance. With further interest in creating a more convenient testing alternative, NAU sought to create a more secure testing environment through greater use of data forensics.

- During the same time frame, Acxiom Corporation amassed a vast database of publicly available personal data. The data are generated from multiple sources, including government agencies and private resources. Acxiom "touches" those data sources up to 3 billion times a day to constantly collect the most up-to-date information that is available. Learning of the challenges faced by institutions offering distance learning programs, Acxiom surmised that the sophisticated service that the company provides to the banking industry might also have applicability in the online environment; thus the two separate organizations joined together in collaborative effort.
- By design, the NAU-Acxiom pilot employed a combination of IAAA features in an effort to realize the goal of user verification. It is acknowledged that, through the standard application process, NAU's students are properly identified through the provision of documentation associated with the steps for admission. Therefore, the first level of the IAAA could be achieved by the university. However, only through the collaborative arrangement could NAU and Axiom expand the task of online student authentication through the integration of expanded personal data that NAU did not have at its immediate disposal. The idea was that students could be required to answer one or more personal questions at various trigger events; including registration, exams, paper submissions, and other significant online course events and work completion events where authentic identity is deemed essential.
- Consistent with the personal information approach used extensively in the financial services industry, the pilot project required each of the operations to supply data representative of the "what we have" and "what we know" protocol in order to verify online student users. The scenario is as follows:

1. In accordance with the Family Educational Rights and Privacy Act, select directory-only data of students who have been properly identified by the university are revealed to Acxiom so that supplemental data can be mined from the company's databases.
2. Participants enter the learner management system (Blackboard CE 6) in a conventional fashion, by use of a unique user name and password issued by the university. Using this detail, students access their assigned course.
3. When entering a trigger event, such as an exam, a series of challenge questions are posed for further authentication. Challenge questions may be posed at any time and frequency during the event. Unanswered or incorrectly answered challenge questions restrict progress to the authorization feature. NAU determines each of the tolerances for challenge questions, including timing, number, and frequency. In addition, NAU decides how to resolve situations when students are not restricted from progress to the authorization feature.
4. Once the examination session has ended, the recorded details of what transpired during each trigger event are disseminated for further review and preliminary scrutiny. This step enables a consequent item analysis of individual questions and responses to the challenge questions, as well as a pass-fail ratio of the group as a whole. Post-course review by the Acxiom and NAU team further ensures that the necessary detail is revealed.
5. Based on an expanded analysis completed collaboratively by NAU and Acxiom, a determination about whether accountability was achieved will be rendered. A summary of students; of type, level, placement, timing, and frequency of challenge questions posed; and of positive (pass) and negative (fail) responses will assist further in the determination of protocol trends while identifying areas for further analysis and corresponding improvements. The results of this accountability feature will be disseminated to interested parties as the review is completed.

As illustrated in this paper, in close collaboration with Acxiom Corporation, the distance learning campus of National American University has piloted a project to further authenticate the identities of online students. The success of this project will advance the credibility of the institution's online delivery options by adding yet another step toward identity verification of online students situated throughout the world. This project is viewed as an example of how corporate and higher learning interests have successfully anticipated and met the challenges encountered as technology and market conditions change and advance.

Frequently Asked Questions

Why Verify Identity?

By verifying identity, we send a message that we are concerned that students receive the deserved credit for the work they are performing. We also demonstrate a proactive interest in compliance with any new requirements requiring a process to verify the identity of the student as being the same as the individual who registered for the course.

Why On Line and Not in Person?

Because of vast expansion of enrollments in online courses, it became increasingly impractical to require students to report to a physical location for scheduled in-person identity verification. Third-party in-person verification of today's contemporary and distributed learner population is logistically difficult, not as secure as desired, and costly.

How Do You Verify the Identity of Online Learners?

We pose questions that require the student to answer with information about their demographics such as where they lived in the past or what type of car they have owned. These questions are called "out of wallet" because they are from the past and the data are not usually found in an individual's wallet. The questions are derived from public data sources and managed by a third party, independent of our institution.

How Do Out of Wallet Challenge Questions Work?

We pose challenge questions at select intervals during a testing session, offering students a predetermined response time to answer the questions.

What Prevents a Student from Having Someone Else Help Answer the Questions?

Our approach is intended to be a barrier to fraudulent activity. While it is clearly not 100 percent safe, it is certainly consistent with practices of today's financial institutions that offer online services. We view this barrier as a sincere beginning to a program that will continue to advance. It is, if nothing else, a notable starting point that meets our current budget and policy requirements.

Why Use an External Data Source to Verify an Individual's Identity?

The volume of data in the U.S. consumer market is larger than any individual academic institution can single-handedly manage. The challenge questions are much more than the typical "what is your mother's maiden name." Because the collection of identifying data is external to the school and not self-directed challenge questions that the student gave to the school, the student can not predict the questions posed. This further increases the integrity of the application.

References

Bruhn, M., M. Gettes, and A. West. 2003. Identity and access management and security in higher education. *EDUCAUSE Quarterly* 26(4): 12–16.

Database of Federal Legislation. http://www.govtrack.us/congress/bill.xpd?bill=h110-4137.

Jeffrey L. Bailie *is Dean of Online Instruction at National American University in Rapid City, South Dakota; and* ***Michael A. Jortberg*** *is Client Executive at Axciom Corporation in Downers Grove, Illinois.*