A Theoretical Approach for Biometrics Authentication of e-Exams

Yair Levy
levyy@nova.edu

Michelle M. Ramim
ramim@nova.edu

Nova Southeastern University, USA

In the past fifteen years the use of Internet technologies has been substantially growing for delivery of educational content. E-learning environments have been incorporated in many universities for the delivery of e-learning courses. However, opponents of e-learning claim that a central disadvantage of such teaching medium is the growing unethical conduct in such environments. In particular, opponents of e-learning argue that the inability to authenticate exam takers is a major challenge of e-learning environments. As a result, some institutions proposed to take extreme measures including asking students to take exams in proctor centers or even abandon completely the offering of e-learning courses in their institutions. This paper attempts to address this important problem by proposing a theoretical approach that incorporates available fingerprint biometrics authentication technologies in conjunction with e-learning environments to curb unethical conduct during e-learning exam taking. The proposed approach suggests practical solution that can incorporate a random fingerprint biometrics user authentication during exam taking in e-learning courses. Doing so is hypothesized to curb exam cheating in e-learning environments.

This paper proposed a theoretical approach for fingerprint biometrics authentication of exam takers in e-learning environments. Teaching via the Internet has become a popular choice for academic institutions (Hiltz & Turoff, 2005). Advances in information systems have enabled educational institutions to implement e-learning systems as teaching environments (Alavi & Leidner, 2001). Furthermore, e-learning has become a powerful medium for academic institutions due to cutting edge technologies. Hiltz and Turoff (2005) noted that e-learning is "the latest of social technologies that ... has improved distance learning" (p. 59).

Gunasekaran et al. (2002) described the growth in e-learning as the "new dynamic learning models…and is leading the [academic] market to a significant paradigm and cultural change" (p. 45). E-learning courses are increasingly offered by universities. Consequently, new resources such as e-books and e-exams have been implemented in e-learning courses. Students' enrollment in e-learning courses has proliferated to over 3 million in the U.S. in 2005 (NCES, 2005). About 82% of those online students were enrolled in undergraduate level courses (NCES, 2005). Accordingly, numerous academic institutions are planning to increase the number of e-learning courses to meet this growth. However, security issues related to e-learning systems have been raised by several scholars (Ramim & Levy, 2006). Moreover, opponents of e-learning argue that the inability to authenticate e-exam takers is one of the major challenges of e-learning. Although there is a major growth in e-learning, some institutions proposed to take extreme measures including asking e-learning students to take e-exams in

proctored centers (Gunasekaran et al., 2002). However, this requirement may not be feasible for e-learning programs with students in remote locations such as in military service or students with severe disabilities.

THEORETICAL BACKGROUND

Unethical Conduct in e-Learning

Given the growth of e-learning, students' unethical conduct in e-learning has become a major concern (Kennedy et al., 2000). Pillsbury (2004) argues that students' unethical conduct has intensified due to technology usage. Most instructors focus on one type of unethical conduct, namely plagiarism (Naude & Hörne, 2006; McCabe, 2003). However, students' unethical conduct encompasses wide array of technology-enabled behaviors such as cheating during e-exam using devices (i.e. PDA, calculator, and cellular phone), engaging in e-collaboration (i.e. instant messenger, chat, and forums), and deceiving (i.e. logging with another student's username/password). These technology-enabled unethical conducts are often undetected by instructors in e-learning courses. Pillsbury (2004) noted several detection mechanisms, such as turnitin.com™, are available to curb plagiarism. Though, extensive body of knowledge is available on plagiarism detections (Decoo, 2002; Hamilton, 2003; Hannabuss, 2001; McLafferty & Foust, 2004), very little attention has been given on providing solutions to other students' unethical conduct such as cheating during e-exams. Pillsbury (2004) noted that detection mechanisms are necessary not only in the initial e-learning portal access. Moreover, additional mechanisms are necessary to authenticate users' access in various e-learning course activities (Newton, 2003). For example, instructors need to verify that e-exam submission is truly performed by the student rather than someone else on their behalf.

According to Center for Academic Integrity (2005), cheating during exams was reported at 74%. In their studies, McCabe and Trevino (1993; 1996) reported 70% of students confessed to cheating on multiple exams. A study by Pincus and Schmelkin (2003) compared faculty members' perceptions on various students' unethical conducts severity. They concluded that faculty members perceived exams' related unethical conduct is one of the most serious unethical behaviors. Similarly, Dick et al. (2002) noted that 24% their study participants believed that "advances on technology have lead … to increase cheating" (p. 173). The perceived severity of exams cheating has led numerous institutions to reduce their e-learning offering or cease e-learning altogether. In fact, Gunasekaran et al. (2002) admitted that inadequate technology has led some institutions to cease offering e-learning courses due to quality concerns of students' assessments and standards. Thus, the central aim of this paper is to propose a conceptual level security solution for this out-braking phenomenon by suggesting a theoretical approach of biometrics authentication to secure e-exams.

Security in e-Learning Environments

Yu and Tsao (2003) discussed security challenges of e-learning environments. However, their exploration focused on shielding the technology infrastructure against unauthorized users. Current security practices in e-learning systems relay principally on the utilization of passwords authentication mechanisms. Similarly, Huang et al. (2004) discussed aspects of security in e-learning systems and

suggested attention to two layers when securing e-learning systems. The first layer addresses security of the technology infrastructure used to facilitate e-learning (i.e. hardware, networks, etc.) and the second layer addresses the various applications employed in enabling e-learning (i.e. learning management systems, rich media communication tools, etc.). Huang et al. (2004) criticized existing proprietary e-learning systems for not paying enough attention to the issue of properly authenticating students, in particular during quizzes and exams. Hugl (2005) noted numerous security related technologies that are not currently employed in e-learning. One such solution can include biometrics technologies that may potentially become an integral part of e-learning systems.

Biometrics Solutions

According to Williams (2002) biometrics is a recognition system that relies on individual humane identities such as DNA, voice, retinal and iris, fingerprints, facial images, and hand prints. Essentially, biometrics technologies operate by scanning a physical characteristic and matching it with the stored data. Williams maintained that fingerprints are the most commonly used biometrics solution as they are less expensive compared with other biometrics solutions. For example, fingerprints are currently used in the Disney® parks and appear to be useful for its high volume traffic and low price authentication. Full hand fingerprint is also used by the U.S. immigration services. Similarly, fingerprints can be used for authenticating students' submissions of e-exams via the use of low cost biometrics devices. Fingerprints can be scanned, transmitted and matched with the aid of a simple device. McGinity (2005) pointed out that biometrics have been commonly employed in replacing conventional password systems.

Yang and Verbauwhede (2003) proposed a secured technique for matching fingerprints in a biometrics system. They argued that biometrics systems enhance security far more than current password systems. Biometrics systems are more accurate as well as simpler to use compared with passwords systems. Coventry, De Angeli and Johnson (2003) discussed the usability aspect of biometrics systems where they argue that there is a "tradeoff between usability, memorability and security" (p. 153). They noted that with the need for increased security passwords are becoming difficult to remember, while fingerprints are a permanent attribute unique to an individual. Yang and Verbauwhede described a fingerprint based biometrics system in which the fingerprint template is kept in a server during initiation. Upon scanning the finger, an input device scans a biometrics signal and transmits it to a server where it is processed for matching. In an effort to shield the system against security compromises, Yang and Verbauwhede recommended encrypting the fingerprint template prior to storing it on the server. Fingerprints templates can be decrypted whenever a matching process occurs.

Fingerprint Biometrics Solutions

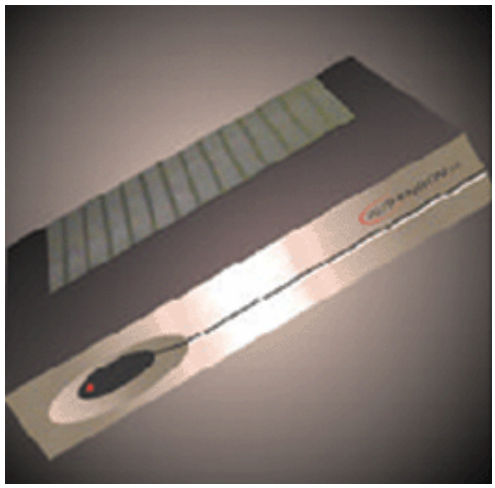
In the past decade the price of biometrics authentication devices has been fallen. Currently there are low cost solutions for biometrics authentication via fingerprint recognition. For example, Figure 1 provides an image a biometrics mouse by JayPeetek Inc. called Scan.U.Match™. This devise is part of a package of fingerprint authentication mechanism. The mouse is about the same size as standard mouse, however, it also has an integrated fingerprint scanner that is managed by client side software and controlled by server side software centralized on an authentication server. Figure 2 provides an

image of Authenteon™, a biometrics authentication server. JayPeetek Inc. claims that their patented Scan.U.Match™ biometrics mouse solution is unique as it "does not capture the finger image and scrambles the algorithm at the point of scan", rather it "creates a 500 byte secure template that cannot be replicated into a user fingerprint" (JayPeetek Inc.). As such, the Scan.U.Match™ is claimed to be highly reliable with "false rejection rate" that is only 0.01%, or 1 out of 100,000 cases.

Figure 1: JayPeetek Inc.'s Scan.U.Match™ Fingerprint Biometrics Authentication Mouse[1]

There are numerous other vendors that offer similar solutions in attractive prices. Examples of some other vendors include SecuGen® Biometrics Solutions (2005) with their OptiMouse III™, onClick® Corp. (2005) with their VIA™ solution, to name a few.

Figure 2: JayPeetek Inc.'s Biometrics Authentication Server, the Authenteon™ Server[2]



Aside from the biometrics fingerprint mouse solutions, there are other biometrics fingerprint solutions including keyboard with fingerprint pad scanner (See Figure 3), PCMCIA fingerprint scanner (See Figure 4), and USB fingerprint token scanners (See Figure 5).

Figure 3: SecuGen®'s Keyboard III™ with fingerprint pad scanners[3]

1 Source: http://www.jaypeetex.com/products/Biometrics/Fingerprints/Scanumatch.htm
2 Source: http://www.jaypeetex.com/products/Biometrics/Fingerprints/Authenteon.htm
3 Source: http://www.secugen.com/products/pk.htm

Figure 4: onClick®'s PCMCIA FingerPrint™ Reader[4]

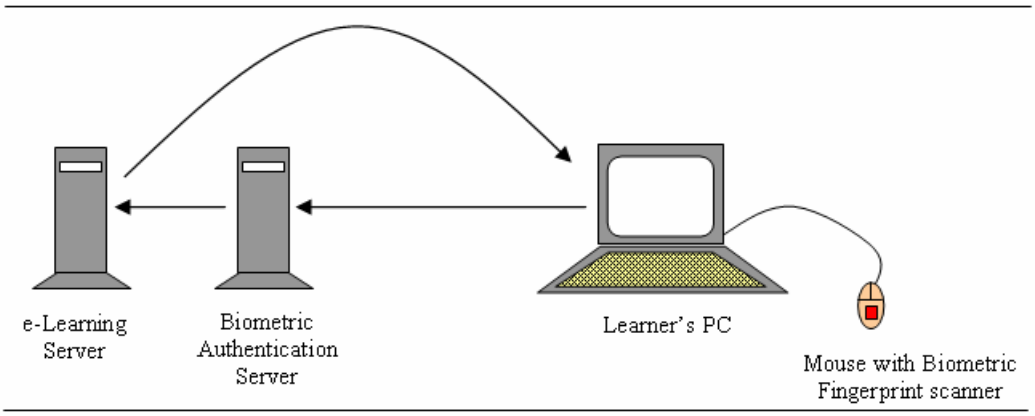
[4] Source: http://www.onclickbiometrics.com/ebusiness/ocbioweb.nsf/wcontent/productsviacard?opendocument

Figure 5: Sony®'s Puppy® Fingerprint Identity Token by Corp[5]

Proposed Theoretical Approach and Recommendations for Future Research

This work proposes a theoretical approach of fingerprint biometrics solution for user authentication during e-exams. Figure 6 demonstrate the proposed conceptual solution. In standard e-exam, the learner's access is authenticated once by the e-learning server at login for the whole duration of the activity session, while the repeated authentication performed is based on the password cashed in the browser. As such, students are able to login to the e-learning server and have someone else take the e-exam on their behalf. The proposed solution will enhance the current authentication process by adding the fingerprint biometrics solution. For example, in WebCT, during e-exam a random fingerprint authentication can occur to validate the e-exam taker. Although not a foolproof approach, requiring the fingerprint authentication of the learner randomly during e-exam with required very short fingerprint scanning response time should provide additional added security. It may discourage learners from having someone else taking the e-exam for them. Therefore, the central claim of this proposed approach is that the incorporation of fingerprint biometrics solution in conjunction with e-learning environments will enable a reduction in exam cheating.

Figure 6: Proposed Fingerprint Biometrics Solution for e-Exam User's Authentication



Unethical conduct, in particular cheating in e-exams was documented in literature as a growing concern by many higher educational institutions. This proposes theoretical approach may add to the

[5] Source: http://bssc.sel.sony.com/Professional/puppy/products.html

general e-learning knowledge by addressing a major issue of e-exam cheating. Future work in this line of research should incorporate this theoretical approach and conduct a study implementing biometrics solutions in e-exams. One example of a study may include comparison of the same instructor teaching two e-learning sections of the same course, where one section will use regular e-exams and the other section will use the fingerprint biometrics approach proposed. The study can propose that:

Proposition 1:

Students taking e-exams using the fingerprint biometrics solution will have lower grades on the e-exam than their counterparts.

Proposition 2:

Students taking e-exams using the fingerprint biometrics solution will take longer time to complete their e-exam than their counterparts.

Results of such study can provide initial investigation in an attempt to address the outgrowing phenomena of unethical conduct in e-exams. Additionally, future research may be fruitful by examining students' attitudes and psychological aspects associated with the proposed solution of e-exam user's authentication. Furthermore, future research may look at the economical issues associated with implementation of such solution.

References

Alavi, M., & Leidner, D. (2001). Research commentary: Technology mediated learning-a call for greater depth and breadth of research. *Information Systems Research, 12*(1), 1-10.

Center for Academic Integrity (2005). Retrieved September 12, 2006, from http://www.academicintegrity.org/cai_research.asp

Coventry, L., De Angeli, A., & Johnson, G. (2003). Usability of large scale public systems: Usability and biometric verification at the ATM interface. *Proceedings of the Conference on Human Factors in Computing Systems.* Florida, USA, 153-160.

Decoo, W. (2002). *Crisis on campus: confronting academic misconduct*. Cambridge, MA: MIT Press.

Dick, M., Sheard, J., Bareiss, C., Carter, J., Joyce, D., Harding, T., & Laxer, C. (2002). Reports from ITiCSE on innovation and technology in computer science education. *ACM SIGCSE bulletin working group, 35*(2), 172-184.

Gunasekaran, A., McNeil, R. D., & Shaul, D. (2002). E-learning: Research and applications. *Industrial and Commercial Training, 34*(2), 44-54.

Hamilton, D. (2003). Plagiarism: Librarians help provide new solutions to an old problem. *Searcher, 11*(4), 26-29.

Hannabuss, S. (2001). Issues of plagiarism. *Library Management, 22*(6/7), 311-319.

Hiltz, S. R., & Turoff, M. (2005). Education goes digital: The evolution of online learning and the revolution in higher education. *Communication of ACM, 48*(10), 59-64.

Huang, W., Yen, D. C., Lin, Z. X., & Huang, J. H. (2004). How to compete in a global education market effectively: A conceptual framework for designing a next generation eEducation system. *Journal of Global Information Management, 12*(2), 84-107.

Hugl, U. (2005). Tech-developments and possible influences on learning processes and functioning in the future. *Journal of American Academy of Business, 6*(2), 250-256.

JayPeetek Inc. (2005). *Scan.U.Match Biometric Authentication System embedded in a mouse*. Retrieved September 12, 2006, from http://www.jaypeetex.com/products/Biometrics/Fingerprints/Scanumatch.htm

Kennedy, K., Nowak, S., Raghuraman, R., Thomas, J., & Dacis, S. (2000). Academic dishonesty and distance learning: student and faculty views. *College Student Journal, 34*(2), 309-315.

McCabe, D. L. (2003, Sep 10). Caught copying: electronic plagiarism is a new addition to the IT lexicon. *Businessline*, 1-3.

McCabe, D. L., & Trevino, L. K. (1996). What we know about cheating in college. *Change, 28*(1), 28-34.

McCabe, D. L., & Trevino, L. K. (1993). Academic dishonesty: honor codes and other contextual influences. *Journal of Higher Education, 64*(5), 522-539.

McLafferty, C. L., & Foust, K. M. (2004). Electronic plagiarism as a college instructor's nightmare-prevention and detection: Cyber dimensions. *Journal of Education for Business, 79*(3), 186-190.

McGinity, M. (2005). Staying connected: Let your fingers do the talking. *Communications of the ACM, 48*(1), 21-23.

Naude, E., & Hörne, T. (2006). Cheating or collaborative work: Does it pay? *Issues in Informing Science and Information Technology, 3*, 459-466.

United States Department of Education, National Center of Educational Statistics (NCES) (2005). *Mini-digest of educational statistics*. Retrieved September 20, 2006, from http://nces.ed.gov/pubs2005/2005017.pdf

Newton, R. (2003). Staff attitudes to the development and delivery of e-learning. *New Library World, 104*(10), 412-426.

onClick® Corp. (2005). Retrieved September 12, 2006, from http://www.onclickbiometrics.com/

Pillsbury, C. (2004). Reflections on academic misconduct: An investigating officer's experiences and ethics supplements. *Journal of American Academy of Business, 5*(1/2), 446-454.

Pincus, H. S., & Schmelkin, L. P. (2003). Faculty perceptions of academic dishonesty: A multidimensional scaling analysis. *Journal of Higher Education, 74*, 196-209.

Ramim, M., & Levy, Y. (2006). Securing e-learning systems: A case of insider cyber attacks and novice IT management in a small university. *Journal of Cases on Information Technology, 8*(4), 24-34.

SecuGen® Biometric Solutions (2005). Retrieved September 12, 2006, from http://www.secugen.com/

Williams, J. M. (2002). New security paradigms. *Proceedings of the 2002 Workshop on New Security Paradigms*, Virginia Beach, Virginia, 97-107.

Yang, S., & Verbauwhede, I. M. (2003). A secure fingerprint matching technique. *Proceedings of the 2003 ACM SIGMM workshop on Biometrics methods and applications*, California, USA 89-94.

Yu, C., & Tsao, C. C. (2003). Web teaching: Design, security, and legal issues. *Delta Pi Epsilon Journal, 45*(3), 191-203.