Using IP Addresses as Assisting Tools to Identify Collusions

Qinghai Gao
Department of Criminal Justice
SUNY at Farmingdale
2350 Broadhollow RD, Farmingdale, NY11735
United States of America

Abstract

Distance Learning has been steadily gaining popularity. More and more universities and colleges are offering online course to increase enrollments. However, one question remains for those who teach online courses: who is doing the real course work? In this paper we will survey the commonly used methods to prevent e-Cheating, look at a few e-Proctors, and illustrate how biometrics is being used for that purpose. In particular we propose a new and alternative method to monitor student activities: using students' IP addresses and timestamps to assist detecting possible cheating behavior. Our results show that IP addresses are applicable to categorize a student as suspect of collusion/cheating during exam. Thus it reduces the number of students an instructor has to pay special attention to for the purpose of preventing dishonesty.

Keywords: Distance learning, Biometrics, Cheating, e-Proctor, Authentication, IP addresses, e-Exam

1. INTRODUCTION

As the Internet becomes an indispensable part of our daily life, Distance Learning has been steadily gaining popularity. A significant portion of the students in the US take online courses. To meet this needs and to attract remote students many colleges and universities offer online courses as replacements or as supplements to the traditional classroom based face-to-face teaching. However, one question remains for those who teach online courses: who is doing the real course work? In particular, online teaching makes it extremely difficult to deal with one serious problem: student dishonesty (Rogers, 2006).

To solve the problem some scholars (Christe, 2003; Rowe, 2004; Apampa, Wills, & Argles, 2009) have proposed a few methods, such as:

- Design open-book exams
- Use discussions, essay, and other written projects; reduce the percentage of exams
- Use a large pool of questions to randomly generate exams for each student
- Require students to take important exams on site

To date the majority of colleges and universities offering online courses use these methods. However, these measures can only alleviate the concern but are not enough to prevent e-cheating since the traditional password-based system is inadequate to authenticate students remotely. For example, one student can ask another student to take an exam for him/her by providing the username and password. One possible solution to the problem is to use biometrics since biometrics cannot be easily transferable between two people.

A few scholars have proposed using biometrics as authentication tools for distance learning. Rabuzin, Baca, & Sajko (2006) and Asha & Chellappan (2008) proposed to combine several different biometric traits in the field of e-learning. Levy and Ramin (2007) proposed approach that can incorporate a random fingerprint for user authentication during e-Exams. Flior & Kowalski (2010) presented a method for providing continuous biometric user authentication in online examinations via keystroke dynamics. Penteado and Marana (2009) proposed using face images captured online by a webcam in the Internet environment to confirm the presence of a user. Alotaibi (2010) proposed using fingerprints for user identification during e-Exams.

In all of these proposals a webcam is required to monitor the activities of a student taking the exam. One implicit requirement is the availability of a high-speed internet connection that constantly transfers biometric information from the location of the test taker to the remote proctor.

Recently a few preliminary products of using biometrics to remotely proctor e-Exams have become available (Lardinois, 2008). However, detailed study and wide adoption of these products have yet to be seen. In this paper we look at the built-in biometric technologies of these products and in particular, we propose a new method to monitor student activities: using students' IP addresses to assist detecting possible cheating behavior.

The rest of the paper is organized as the following. In Section 2 we will introduce how biometric system works and describe a few commonly used biometrics for e-Learning. Section 3 introduces three commercially available products designed for proctoring e-Exams. In Section 4 we show the results of monitoring students IP Addresses to estimate possible cheating behavior during exams. Lastly, Section 5 will summarize the paper and propose future research direction.

2. BIOMETRIC AUTHENTICATION

Biometrics is defined as the identification of an individual based on physiological and *behavioral* characteristics. Commonly used physiological characteristics include face (2D/3D facial images, facial IR thermo-gram), hand (fingerprint, hand geometry, palmprint, hand IR thermogram), eye (iris and retina), ear, skin, odor, dental, and DNA. Commonly used behavioral characteristics include voice, gait, keystroke, signature, mouse movement, and pulse. And two or more of the aforementioned biometrics can be combined in a system to improve the recognition accuracy. In addition, some soft biometric traits like gender, age, height, weight, ethnicity, and eye color can also be used to assist in identification.

Generally a biometric system is designed to solve a matching problem through the live measurements of human body features. It operates with two stages. First, a person must register a biometric in a system where biometric templates will be stored. Second, the person must provide the same biometric for new measurements. The output of the new measurements will be processed with the same algorithms as those used at registration and then compared to the stored template. If the similarity is greater than a system-defined threshold, the verification is successful; otherwise it will be considered unsuccessful. Due to the fuzzy measurements of biometrics an error-correction coding is needed. Table 1 (Refer to Appendix) lists a few biometrics and their features for identification and/or authentication.

Table 1 Biometric features for authentication

Biometrics	Identifying Features	Error Correction	Reference
Keystroke	Duration, latency: a computer user's typing patterns consist of durations for each letter typed and latencies between keystrokes	Discretization	Monrose, Reiter, & Wetzel, 1999
Voice	Text-dependent or text-independent speaker utterance units	Discretization	Monrose, Reiter, Li, & Wetzel, 2001
Signature	Dynamic signature features, such as pen-down time, max forward *Vx* (Velocity in x direction), max backward *Vy* (velocity in y direction), time when the last peak of *Vx* or *Vy* occurs, pressure, height-to-width ratio, and so on.	Averaging	Hao, & Chan, 2002
Face	Facial features: positions, sizes, Angles, etc	RS code	Chen & Chandran, 2007
Iris	Digital representation of iris image processed with Gabor wavelet	RS code Hadamard	Hao, Anderson, & Daugman, 2005
Fingerprint	Minutiae points: ridge ending and ridge bifurcation	Quantization	Uludag, Pankanti, & Jain, 2005
Palmprint	Unique and stable features such as principal lines, wrinkles, minutiae, delta points, area/size of palm	RS code	Kumar & Kumar, 2008

Not only is biometrics being proposed as the required authentication methods for college students who take online courses, many online certification programs also start using biometrics for authentication. For example, the defensive driving course provided by American Safety Council requires course taker to choose one of two traits for authentication during the training: voice or keyboard typing biometrics.

To register the chosen biometric a training session is conducted before the formal course starts. If voice is selected, the taker needs to read a sentence multiple times; if the keyboard typing is selected, the taker needs to type a sentence for a few times. The training session ends once a user registered his/her chosen biometric successfully. Then the formal course starts. In the duration of the course the system will ask the test taker to provide the same biometric at random times.

In fact, for better security it is necessary to ask students to provide two or more biometrics instead, though it may cause more inconvenience. Currently, two proposed behavioral biometrics, keystroke and mouse clicking, can be used together to provide continued authentication. However, false recognition rate can be very high for behavior biometrics if a user has sudden changes in these behaviors. Therefore, a better choice would be using a relatively more stable physiological trait, such as fingerprint or face, with a behavioral trait.

3. COMMERCIAL E-PROCTORS

At least three products have been adopted by some colleges and universities for their online courses (Lardinois, 2008). The first one is named *Secureexam*, a remote proctor made by *Software Secure*; The second one is named *Webassessor*, made by *Kryterion*; and the third one is named *ProctorU*, made by *Axicom*. A brief description of each product is followed. Refer to Table 2 for more details about these products.

Table 2 Commercial e-Proctors (Lardinois, 2008)

Name	**Securexam**	**Webassessor**	**ProctorU**
Description	Securexam Remote Proctor, a small device which features a fingerprint scanner, microphone, and a video camera with a 360 degree view. To start an exam, students need to provide their fingerprints for identification. During the exam, the microphone and video look out for anything suspicious like an unknown voice or movement on the camera.	Kryterion's Webassessor uses face image captured by webcams, and keystroke biometrics (typing styles) captured by software to authenticate the test taker and alerts the proctors if there is a change when somebody else has taken over	The system gathers some personal data from a variety of databases, including criminal files and property records, and uses the data to ask students a few questions, such as address, employers, etc. Students need to answer the questions correctly before they can start the exams. In order to use ProctorU, each student also needs to reserve a time slot for an exam and has a webcam ready that can monitor the exam environment. With a webcam a human proctor would remotely guide a student in the process of starting an exam.
College	Troy University, New York University	Penn State University	National American University
Cost	$150 per student	$50~$80 per student	$10 per student
Company	*Software Secure Inc*.	*Kryterion Inc*.	*Axicom Corp*.
Web	www.softwaresecure.com	www.kryteriononline.com	www.proctoru.com

Overall, these products provide educators with technological options to combat e-Cheating by combining both conventional password-based authentication with modern biometrics-based authentication. We anticipate that more and more universities and colleges would adopt these products. Hopefully there will be legislature to mandate the adoption of these products for all institutions offering online courses in the near future. However, it is necessary to seek alternative tools and methods to detect e-Cheating before that becomes a reality.

4. USING IP ADDRESSES and TIMESTAMPS AS MONITORING TOOLS

To take online course each student has to acquire a computer for internet access. Theoretically, each computer has a unique IP address which identity a specific computer on the Internet. Currently in US, IPv4 (Internet Protocol version 4) are running on all the computers in nearly all the educational institutions. One example of the IP address: 132.168.123.127. In Windows operating system, one can look at the IP address of a computer by going to the Command Prompt and typing the command in quote: “IPCONFIG /ALL”. In Linux operating system the corresponding command is “ifconfig”.

By surveying students taking online courses, we found that they typically use computers from three different locations: home, campus, and work. The majority of students typically use computers at home or on campus. Some of them may take tests in a hotel during business trips. However, for taking important tests rarely would someone use wireless network while on the run, such as taking an exam on a train. For students on campus our findings are also based on the following facts we discovered: (1) most universities and colleges use public IP addresses for their computers, which means each computer has its own routable IP address. It is not the case that multiple computers share a same IP address simultaneously. NAT (Network Address Translation) are rarely used on campus. (2) Although DHCP is widely used, the campus computers in a computer lab or in a dormitory have relatively stable and similar IP addresses. Based on this fact it is not impossible to check if two students from the same class started the same test at a nearby location around the same time.

For students at home we found that they might use private IP addresses within their home-based local area network. However, the public IP address from an ISP is rarely changed for a student. The chance that two students from the same family or location take the same online course is extremely small. With these findings we believe that IP addresses together with timestamp can be used as an indicator of possible cheating behavior during important exams. At a minimum they can help an instructor to pinpoint the suspects of cheating. With the online teaching software system *Angel* from Blackboard Inc, which automatically records the IP address and timestamps upon signing in, we carried out research for a few online courses we were teaching. The results are given below.

Table 3 Computer IP addresses at which students took the exams

	IP addresses			
Student #	Exam 1	Exam 2	Exam 3	Exam 4
1	74.101.140.139	74.101.140.139	74.101.140.139	74.101.140.139
2	24.45.42.13	24.45.42.13	24.45.42.13	24.45.42.13
3	137.125.41.85	137.125.41.20	Absent	24.189.53.97
4	69.112.216.162	69.112.216.162	69.112.216.162	69.112.216.162
5	137.125.192.210	137.125.192.210	137.125.192.210	137.125.192.210
6	68.194.1.160	24.185.168.110	68.194.1.160	24.185.168.110
7	96.232.164.11	96.232.164.11	96.232.164.11	96.232.164.11
8	**24.191.210.158**	**96.224.66.137**	**24.191.210.158**	**137.125.245.20**
9	**24.191.210.135**	**96.224.66.137**	**24.191.210.135**	**137.125.245.15**
10	98.116.170.141	Absent	98.116.97.40	98.116.97.40
11	98.113.40.77	98.113.40.77	98.113.40.77	98.113.40.77
12	68.194.255.201	68.194.255.201	68.194.255.201	68.194.255.201
13	69.112.24.82	69.112.24.82	69.112.24.82	69.112.24.82

In Table 3 we listed the IP addresses of 11 students each of whom took four exams and those of 2 students (#3 & #10) who only took three exams due to absences. 8 of the 11 students (#1, #2, #4, #5, #7, #11, #12, & #13) always took the exams from the same IP addresses. Student #6 took Exam 1 and Exam 3 from one IP address and Exam 2 and Exam 4 from another IP address. Surprisingly, student #8 and #9 took the each of the four exams from either very similar or the same IP address. Therefore, we labeled these two students as suspects of cheating during the exams.

We conducted further examination on student #8 and #9 by listing their submission times for the four exams. The results are given in Table 4. Also we find out the geographical locations of the five IP addresses with IP Tracer, as given in Table 5. Based on the information in Table 4 and Table 6 we proposed possible cheating scenarios for these two students, as given in Table 6. Since students are required to take these exams independently, i.e., without seeking help from anyone else, all these four scenarios are considered cheating.

Table 4 IP addresses & timestamps of two suspects

	IP addresses & Timestamps			
Student #	Exam 1	Exam 2	Exam 3	Exam 4
8	24.191.210.158	96.224.66.137	24.191.210.158	137.125.245.20
Submission Time	9/1/10 17:40	10/12/10 11:39	11/16/10 13:06	12/13/10 20:15
9	24.191.210.135	96.224.66.137	24.191.210.135	137.125.245.15
Submission Time	9/1/10 16:26	10/12/10 9:00	11/16/10 13:45	12/13/10 20:13
Time Difference	1 hour 14min	2 hour 39 min	39 min	2 min

Table 5 Geographical locations of the suspected IP addresses

IP address	24.191.210.158	24.191.210.135	96.224.66.137	137.125.245.20	137.125.245.15
IP country code	US	US	US	US	US
IP state	New York	New York	New York	New York	New York
IP city	West Babylon	West Babylon	Medford	Farmingdale	Farmingdale
IP postcode	11704	11704	11763	11735	11735
IP latitude	40.7067	40.7067	40.8314	40.7334	40.7334
IP longitude	-73.3501	-73.3501	-72.9758	-73.4281	-73.4281
ISP of this IP	Optimum	Optimum	Verizon	FSC	FSC

Table 6 Possible cheating scenarios for student #8 and #9

	Possible cheating scenarios
Exam 1	Two students took the exam side-by-side in the same household, helping each other. They may share one copy of the textbook; Student #8 finished the exam 1hr 14min earlier than student #9.
Exam 2	The exams were done with the same computer. Since student #8 finished the exam 2hr 39min earlier than student #9, there is possibility, student #8 did the exam for student #9.
Exam 3	Similar to Exam 1, except student #9 finished the exam 39min earlier than student #8.
Exam 4	Two students took the exam side-by-side in the computer lab of school, helping each other. And they finished the exam almost at the same time.

5. CONCLUSION

In this paper we listed the commonly used methods to prevent e-Cheating and recognized the inadequacy of using them to achieve the goal of eliminating student dishonesty in Distance Learning. We looked at how biometrics can provide a solution to the problem and surveyed the existing proposals of using biometrics to authenticate remote students. We looked into three commercially available products that have been tested by some universities to proctor e-Exams. Above all we proposed a new method of using IP addresses to single out cheating suspects for online exams. Our results show that the method is effective at identifying student collusion during exam.

6. REFERENCES

Alotaibi, S. (2010). Using Biometrics Authentication via Fingerprint Recognition in E-exams in E-Learning Environment. *The 4th Saudi International Conference*, The University of Manchester, UK.

Apampa, K., Wills, G., & Argles, D. (2009). Towards Security Goals in Summative E-Assessment Security. *International Conference for Internet Technology and Secured Transactions*, pp: 1-5.

Asha, S., & Chellappan, C. (2008) Authentication of e-learners using multimodal biometric technology. *International Symposium on Biometrics and Security Technologies*, pp: 1-6.

Chen, B., & Chandran, V. (2007). Biometric Based Cryptographic Key Generation from Faces. *Proc. of the 9th Biennial Conference of the Australian Pattern Recognition Society on Digital Image Computing Techniques and Application*, pp: 394–401.

Christe, B. (2003). Designing online courses to discourage dishonesty. *Educause Quarterly*, 4:54-58.

Flior, E., & Kowalski, K. (2010) Continuous Biometric User Authentication in Online Examinations, *Seventh International Conference on Information Technology,* pp: 488-492.

Hao, F., & Chan, C. (2002). Private key generation from on-line handwritten signatures. *Information Management & Computer Security*, 10(2): 159–164.

Hao, F., Anderson, R., & Daugman, J. (2005). Combining cryptography with biometrics effectively. *Technical Reports*, University of Cambridge, Computer Laboratory.

Kumar, A., & Kumar, A. (2008). A palmprint-based cryptosystem using double encryption. *Proc. of SPIE*, 6944:1-9.

Lardinois, F. (2008). The Proctor at Home: Using Technology to Keep Online Students from Cheating. Available at:
http://www.readwriteweb.com/archives/

Levy, Y., & Ramin, M. (2007) A Theoretical Approach for Biometrics Authentication of e-Exams. Available at:
http://telem-pub.openu.ac.il/users/chais/2007/morning_1/M1_6.pdf

Monrose, F., Reiter, M., & Wetzel, S. (1999). Password Hardening Based on Keystroke Dynamics. *Proc. of the ACM Conference in Computer and Communications Security*, pp: 73–82.

Monrose, F., Reiter, M., Li, Q., & Wetzel, S. (2001). Cryptographic key generation from voice. *Proc. of the IEEE Symposium on Security and Privacy*.

Penteado, B., & Marana, A. (2009). A Video-Based Biometric Authentication for e-Learning Web Applications. *Enterprise Information Systems. Lecture Notes in Business Information Processing*, 24(IV): 770-779.

Rabuzin, K., Baca, M., & Sajko, M. (2006). E-learning: Biometrics as a Security Factor. *International Multi-Conference on Computing in the Global Information Technology*, pp: 64.

Rogers, C. (2006). Faculty perceptions about e-cheating during online testing. *Journal of Computing Sciences in Colleges*, 22(2): 206-212.

Rowe, N. (2004). *Online Journal of Distance Learning Administration*. Available at:http://www.educause.edu/Resources/CheatinginOnlineStudentAssessm/153159.

Uludag, U., Pankanti, S., & Jain, A. (2005). Fuzzy Vault for Fingerprints. *Proc. of Audio and Video-based Biometric Person Authentication*, pp: 310-319.