Profile Based Student Authentication in Online Examination

Abrar Ullah
School of Computer Science,
University of Hertfordshire, Hatfield, UK
a.ullah3@herts.ac.uk

Dr.Hannan Xiao, Dr. Mariana Lilley
School of Computer Science,
University of Hertfordshire, Hatfield, UK
h.xiao, m.lilley {@herts.ac.uk}

Abstract— **Online examination is an increasingly important component of online courses, and student authentication is widely seen as one of the major concerns for online examinations. In the online examination scenario, face-to-face supervision is absent, and students may attempt to use third party to increase their score. The paper aims to investigate authentication challenges to online examinations, review benefits and constraints of existing authentication traits, and discuss alternative techniques. We propose the use of profile based authentication framework (PBAF) together with user-id and password for the authentication of students during online examinations. The proposed solution utilizes profile based challenge questions and user-id and password, which is verified by development of PBAF in a virtual learning environment.**

Keywords—Authentication, online examination, e-learning, profile, challenge questions

I. Introduction

Online learning has evolved teaching and learning from a conventional class room into a valuable educational resource accessible from all geographical locations beyond physical boundaries. The online learning environments are accessible, available, updatable, resource efficient, useable, economical [19] and therefore, widely adopted by a number of educational institutions in various disciplines.

Online learning integrates teaching, learning and examinations. In the scenario of online examinations, there may be no face-to-face interaction between the students, tutors and administrators [10], thus, security is vital to the credibility of awards granted using online learning environment. As in [15], the nature of online learning environment makes it more vulnerable to various security threats. Online examinations can be high stake applications and may fall to impersonation and malicious attacks for higher grades [3]. One of the primary goals of authentication is to ensure genuine interaction of student with the online examination. The conventional user-id and password is not enough to verify identity of an online student. This paper discusses existing authentication features, and review their benefits and constraints.

A profile based authentication technique is proposed to be used in addition to user-id and password technique. We have designed profile based authentication framework in a virtual learning environment. The proposed solution uses profile questions for building student profile over time. The profile information is used to generate challenge questions, which supports student authentication during online examinations.

II. Online Examination

Examination is a fundamental and integral component of online learning environments. With the development of learning technologies, assessment has also evolved. The online examinations may include questionnaires, assignments, projects, peer review, essays, quizzes, self assessment and portfolios [13]. The students interact with online learning environment remotely by virtual means and hence, building confidence and trust is of vital importance[14].

A. Summative Assessment:

Summative assessments evaluate the learning outcomes. The student's skills are measured against the learning goals using a set of assessment techniques. The summative assessment may be one or a combination of multiple assessment activities in the online examination. The online examination or summative assessment may attract threats from the students due to high stakes.

B. Formative Assessment:

The teachers or supervisors use formative assessment to review feedback on learner's activities [6] and record progression. In the online learning environment, it may use the same assessment components as summative assessment. However, it may not accumulate toward the final result, which minimises security threat to formative assessment.

III. Authentication

Authentication attempts to verify that the user is who he claims to be. In online examination scenario, it aims to verify identity of online students and plays a key role in security. Unlike face-to-face examination, authentication in online examination is not supervised and invigilation is largely different in an uncontrolled remote environment [17]. Authentication guarantees currency of online examination, as the legitimate interaction between student and online examination is more likely to lead to authentic results.

This Research is sponsored by Wales Deanery Cardiff

A. *Knowledge Based Authentication*

As in [17] , knowledge based authentication verifies identity on the basis of “what you know”. It requires personal knowledge to authenticate individual access to online environments. A user-id and password scheme is a commonly used example. It is a popular authentication method [7], because, passwords are key to authentication and easy to remember. In a situation, e.g. banking, where users are highly likely to make every effort to prevent illicit access, this scheme can be effective. However, due to the nature of online examinations, the students may conveniently share their login credentials with third party to boost their grades. As in [11], low entropy passwords are prone to dictionary attacks. Hence, online examinations relying on user-id and password are susceptible to collusion and malicious attacks.

Challenge questions or security questions are another example of knowledge based authentication. It is generally used in banking sector [18] for authentication, and corporate email service providers for credential recovery [20]. We will discuss incorporation of challenge questions in online learning in section-IV.

B. *Object Based Authentication*

In a similar vein, individuals in possession of identity objects are believed to be authentic. The users are identified by presenting or applying physical objects i.e. electronic chip cards, magnetic cards, and digital keys. It is broadly used in banking sector, transportation and secure premises access. The identity objects benefit from storage of automated identity print onto electronic and magnetic chips. In the online examination scenario, presence of both entities i.e. identity objects and student, maximizes the security. However, objects may be transferred to a third party or compromised, which poses potential threat to online examinations [4] i.e. collusion. In addition, it may require special purpose devices to take user input for registration and authentication.

C. *Biometrics or Characteristics Based Authentication*

The biometrics or characteristics based authentication is performed by the verification of individual’s physical or behavioural characteristics [5]. Biometric frees individuals from remembering passwords and carrying cards as the person is the key for identification [9]. A number of biometric authentication features have evolved from recent research and implemented in online learning systems including finger print, video authentication, face recognition, audio recognition or combination of these features in the form of multi-modal biometrics.

Fingerprint is one of the most commonly used biometrics authentication features [2], which offers unique global identifier. The fingerprint may offer secure solution and minimize threat of impersonation in online examinations. The wider implementation of fingerprint for online examination requires additional resources i.e. fingerprint scanners and software on the client’s location.

Face recognition biometric trait implements image recognition and pattern matching algorithms to verify user identity [22]. It may be a reliable authentication candidate for online examinations. However, face recognition biometric may not be secure authentication for online learning system due to complexity of face recognition technology [3]. Various aspects such as variable face expression, capture point direction, variable light, environment, web camera, weather and other pertinent accessories e.g. beards, glasses can affect the authentication results.

The audio or voice biometric is used both for speech recognition and speaker identification. In this biometric trait, human voice is recognized using automated system based on the data from speech wave. As in [10], intra-individual variations i.e. human voice features like acoustic, voice pitch and speaking style or accent provide a unique identifier for use as a behavioural feature. As a behavioural authentication feature, it may be a secure authentication to shield online examination. However, varying speaking speed, environmental noises, quality of recording equipments may not result in robust outcome [21]. The intra-individual variation can be a major practical issue in voice recognition. In the context of online learning user training can be an overhead, when recording voice samples during the enrolment and authentication phase. The user’ voice may be recorded for use in replay attacks as the ‘liveness’ of a user can not be verified [8].

Signature verification is a legacy feature and it has been widely used and highly acceptable in day to day life transactions [1]. However, as in [16], the evolution of technology has enabled capture and verification of human signature using a combination of computer software and hardware. It is unique behavioural trait and a potential candidate for user authentication. Purpose built accessories like digital signature pads, tablets and digital pens are used to capture signature information [1]. It may not be easily replayed as other biometric features and signature may only be stamped by the individual user. However, signature recognition may face issues i.e. complexities of algorithms, variation in signatures on different occasions, individual’s emotional and physical influence on signature and signature forgery [12].

The biometric authentication has its strengths and limitations in terms of usability, cost and security when used in online examinations. It ensures presence of the individual students by verifying physical and behavioural characteristics, which can be a preferred way to counter impersonation. However, it may incur additional cost for using special purpose hardware and software kits, and its wider implementation globally could be a challenge. Unlike knowledge based authentication, the biometrics features are not amendable and hence not useable if compromised. Some biometric features may require student training and additional administration to facilitate and monitor various processes. The outcome of biometric traits may be affected by variation in human physical and environmental atmosphere, minimising authentication accuracy.

IV. PROFILE BASED AUTHENTICATION

The proposed solution, Profile Based Authentication Framework (PBAF) uses multi modal authentication approach to secure online examination. The solution comprises of two

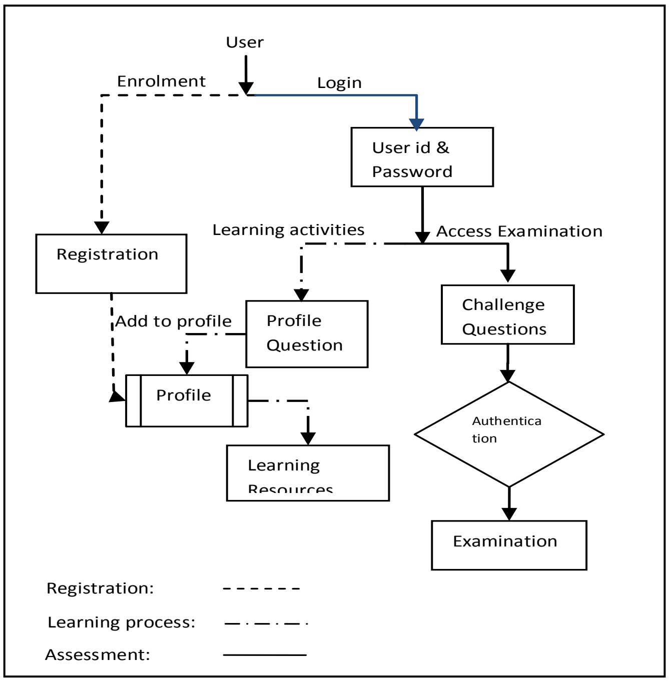


Figure 1. Profile Based Authentication Framework

layers of authentication i.e. user-id and password, and challenge questions. Initially user-id and password can be used to login into the online learning environment to carry out regular learning activities. During the learning process, students are posed profile questions that are used to extend and refine individual student profile. When a student requests to access online examination, the second layer of authentication triggers challenge questions generated from student's profile. Profile questions are used to collect answers in order to built and update student profile. Challenge questions are used to verify student identity. The primary focus of the proposed solution is secure authentication for online examination or summative assessment. "Fig. 1" demonstrates the PBAF solution.

A. *Profile*

The profile is a student's description in the form of questions and related answers. It represents a student by using information received from questions and answers during registration and learning process. The questions and answers in a student profile can be collected pertaining personal information, education, activities, professional experience, hobbies, future objectives, and learning activities.

B. *Profile Questions*

The profile questions are presented to students in order to capture additional information to extend and refine profile. The student is required to provide user-id and password to pass through initial authentication to access the online learning environment. The student is queried to supply answers to profile questions on each visit to be able to access the learning resources. Answers to profile questions received during the learning process are used to extend profile. This is a recurrent process and binds to student session and date.

C. *Challenge Questions*

The challenge questions are randomly picked from individual profile, when a student requests to access summative assessment. The PBAF generates and presents unpredictable challenge questions during authentication. When the challenge questions are answered, the framework invokes authentication process to verify student's identity against profile answers.

D. *Authentication*

The students are allowed access to online examination by providing correct answers to the challenge questions based on the student profile. The students failing to supply correct answers are denied access to online examinations.

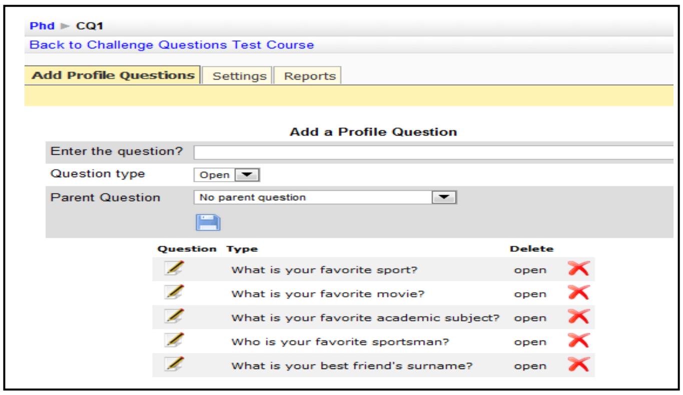
V. THE DESIGN AND IMPLEMENTATION OF PBAF

The proposed solution is designed and developed on Modular Object Oriented Distributed Learning Environment (MOODLE). Moodle is an open source online learning environment developed in PHP and MySQL database.

The PBAF solution is developed as a moodle block, which can be deployed automatically by copying the development files in the block directory and visiting the notifications link in the administration panel. It is a version controlled module and amendable on the running systems. The deployment module adds PBAF tables i.e. questions, profile, authentication, registration and administration. The tables are linked to the core moodle table "users" by using foreign key relation. The framework is configurable, which can be added, removed, and deactivated by the system administrator.

A. *Administrator Scenario*

Only the administrator can access configuration of PBAF block for administration. In the configuration panel, questions can be added, amended and deleted to the questions library. The question library is used for posing profile questions. The PBAF authentication can be configured and linked to the desired assessment modules e.g. lessons, quizzes, forums etc. The profile questions can be set to popup on a user session or date. The number of questions can also be configured both for profile and challenge questions. We have given some student scenarios to explain working of the framework. "Fig. 2"shows the administrator scenario.


Phd ► CQ1

Back to Challenge Questions Test Course

Add a Profile Question

Enter the question?

Question type: Open

Parent Question: No parent question

Question	Type		Delete
✎	What is your favorite sport?	open	✗
✎	What is your favorite movie?	open	✗
✎	What is your favorite academic subject?	open	✗
✎	Who is your favorite sportsman?	open	✗
✎	What is your best friend's surname?	open	✗

Figure 2. Administrator scenario

B. Student Registration Scenario

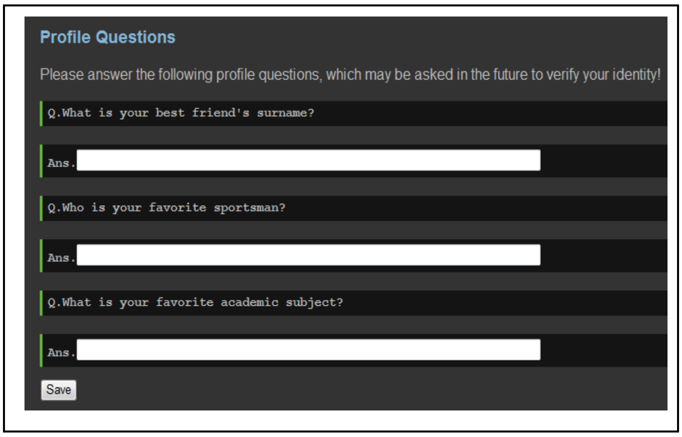
On the very first login, the students are directed to a registration form to collect personal, educational, support, and employment information. This information is processed and added to the student profile in the form of questions and answers e.g. student date of birth into "what is your year of birth", "what is your month of birth".

C. Student Profile Questions Scenario

As part of their regular interaction with the course, students are required to enter their user-id and password to access their courses. As in "Fig. 3 ", on login to the course, student is directed to provide answers to profile questions in order to access the learning resources. When the profile questions are answered, the information is stored in the student profile. This is a recurrent profile building process all the way through the learning process.

D. Student Challenge Questions Scenario

The PBAF can be linked to some or all available assessments on a moodle course by the administrator. On request to an assessment, the framework directs a student to challenge questions page for authentication as in "Fig. 4". The challenge questions are selected randomly by the system from student profile. The student is granted access, if correct answers to the challenge questions are received. The student is barred from access to assessment if fails to authenticate. The student account can only be unbarred by the course administrator.



Profile Questions

Please answer the following profile questions, which may be asked in the future to verify your identity!

Q.What is your best friend's surname?

Ans.

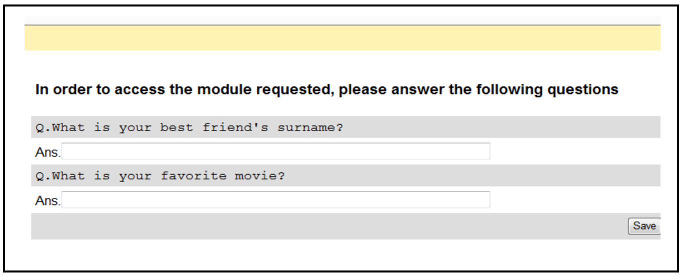
Q.Who is your favorite sportsman?

Ans.

Q.What is your favorite academic subject?

Ans.

Figure 3. Profile Question Scenario



In order to access the module requested, please answer the following questions

Q.What is your best friend's surname?

Ans.

Q.What is your favorite movie?

Ans.

Figure 4. Challenge Questions Scenario

VI. CONCLUSION

The popularity and growth of online learning has also begun to raise serious security concerns. The threats to online examination can challenge the credibility of online learning approach. The stakes are mainly different in the online examination and conventional authentication approaches cannot be enough to counteract collusion and malicious attacks. This paper reviewed various authentications traits, its feasibility in the online learning environment, and strengths to deal with collusion and malicious attacks. We have presented a knowledge based solution for authenticating online learning users by exploiting user-id and password, and challenge questions. Our approach uses a set of questions to create students profile during registration and learning activities. The question library is generic and can be customised across various disciplines and institutions. In our approach, the profile build-up is a continuous process during the learning timeline. The student requires supplying user-id and password for initial login, and examination can be accessed by supplying correct answers to the challenge questions randomly picked from profile. Unlike biometrics approach, our solution doesn't require special purpose input accessories and computational resources. This approach minimises threats of collusion and malicious attacks to online examination by generating random questions from a heap of questions from a student's profile. It may be difficult for student to remember all the challenge questions and pass on profile information to a third party.

In the proposed solution, the numbers of challenge and profile questions are defaulted to three and two. Future work would therefore, concentrate to identify the number of posing questions and a traffic light scheme for authentication.

REFERENCES

[1] Adamski M., Saeed K. Online Signature Classification and its Verification System. 7th Computer Information Systems and Industrial Management Applications. 2008:189-94.

[2] Aggarwal G., Ratha N., Jea T. Y., Bolle R., editors. Gradient based Textural Characterization of Fingerprints. Biometrics: Theory, Applications and Systems; 2008: IEEE.

[3] Agulla E. G., Rifón L. A., Castro J. L. A., Mateo C. G., editors. Is My Student at the Other Side? Applying Biometric Web Authentication to E-Learning Environments. Eighth IEEE International Conference on Advanced Learning Technologies; 2008: IEEE.

[4] Apampa K. M., Wills G., Argles D., editors. An approach to presence verification in summative e-assessment security. International Conference on Information Society (i-Society 2010); 2010: IEEE.

[5] Asha S., Chellappan C., editors. Authentication of e-learners using multimodal biometric technology. International Symposium on Biometrics and Security Technologies 2008: IEEE.

[6] Birenbaum M. Assessment 2000: Towards a pluralistic approach to assessment. Alternatives in

assessment of achievements, learning processes and prior knowledge. 1996:3-29.

[7] Das M. L., Saxena A., Gulati V. P. A dynamic ID-based remote user authentication scheme. Consumer Electronics, IEEE Transactions on. 2004;50(2):629-31.

[8] Eveno N., Besacier L., editors. Co-inertia analysis for liveness test in audio-visual biometrics. Proceedings of the 4th International Symposium on Image and Signal Processing and Analysis; 2005: IEEE.

[9] Gil C., Castro M., Wyne M., editors. Identification in web evaluation in learning management system by fingerprint identification system. Frontiers in Education Conference (FIE); 2010: IEEE.

[10] Hayes B., Ringwood J., editors. Authenticating student work in an e-learning programme via speaker recognition. 3rd International Conference on Signals, Circuits and Systems (SCS) 2009: IEEE.

[11] Huiping J., editor. Strong password authentication protocols. 4th International Conference on Distance Learning and Education (ICDLE); 2010: IEEE.

[12] Jazahanim K. S., Ibrahim Z., Mohamed A., editors. Online zones' identification using signature baseline. Second International Conference on the Applications of Digital Information and Web Technologies; 2009: IEEE.

[13] Joosten-Ten Brinke D., Van Bruggen J., Hermans H., Burgers J., Giesbers B., Koper R., et al. Modeling assessment for re-use of traditional and new types of assessment. Computers in Human Behavior. 2007;23(6):2721-41.

[14] Karvonen K., editor. Creating trust. In Proceedings of the Fourth Nordic Workshop on Secure IT Systems; 1999: Citeseer.

[15] Mcmurtry K. E-Cheating: Combating a 21st Century Challenge. THE journal. 2001.

[16] Meshoul S., Batouche M., editors. Combining Fisher Discriminant Analysis and probabilistic neural network for effective on-line signature recognition. 10th International Conference on Information Sciences Signal Processing and their Applications (ISSPA); 2010: IEEE.

[17] Moini A., Madni A. M. Leveraging Biometrics for User Authentication in Online Learning: A Systems Perspective. IEEE Systems Journal. 2009;3(4):469-76.

[18] Rabkin A., editor. Personal knowledge questions for fallback authentication: Security questions in the era of Facebook. In SOUPS 2008: Proceedings of the 4th Symposium on Usable Privacy and Security; 2008; 23, New York, NY, USA: ACM.

[19] Ruiz J. G., Mintzer M. J., Leipzig R. M. The impact of e-learning in medical education. Academic medicine. 2006;81(3):207.

[20] Schechter S., Brush A. J. B., Egelman S., editors. It's No Secret. Measuring the Security and Reliability of Authentication via. 30th IEEE Symposium on Security and Privacy; 2009: IEEE.

[21] Shaver C. D., Acken J., editors. Effects of equipment variation on speaker recognition error rates. International Conference on Acoustics Speech and Signal Processing (ICASSP); 2009: IEEE.

[22] Zhao Q., Ye M., editors. The application and implementation of face recognition in authentication system for distance education. 2nd International Conference on Networking and Digital Society (ICNDS); 2010: IEEE.