An Interactive and Secure E-Examination Unit (ISEEU)

A Proposed Model for Proctoring Online Exams

Yousef Sabbah, Imane Saroit and Amira Kotb
Information Technology Department
Faculty of Computers and Information, Cairo University
Cairo, Egypt
ywsys@hotmail.com, iasi63@hotmail.com, a_kotb10@yahoo.com

***Abstract*— This paper proposes a new approach for e-assessment or e-examination authentication. This approach enables educational institutions to conduct cheating-free e-examinations, which has been considered a big challenge of e-learning within the previous decade. It ensures that an examinee is the correct student throughout his exam. This approach provides virtual, interactive, and secure e-examination sessions. A prototype will be developed on Moodle with a media server to broadcast sessions. A control toolbox will be developed to provide interaction between a proctor and examinees. An e-exam can not be started without approval by a proctor who can also pause, resume or terminate an e-exam any time if an examinee violates examination instructions.**

Keywords*— *Authentication; Cheating; e-Assessment; e-Examination; e-Learning; Examinee; Proctor; Security.

I. INTRODUCTION

One reason for unsuccessful e-learning is the lack of completely trusted, secure and protected e-assessment [1-7]. Around 73.6 percent say that cheating is easier in an e-examination than in its traditional counterpart [7]. Therefore, several evaluation studies recommended that security issues in e-assessment should be resolved [8, 9]. This paper contributes in resolving this vital issue by introducing an efficient and highly secure model for proctoring online exams. The rest of this paper is divided into five sections. Section II explores the various user authentication methods and discusses their drawbacks. Section III, on the other hand, presents the different schemes of e-assessment authentication and defines the essential types of impersonation threats. In section IV, the proposed model is presented and its algorithm is illustrated and discussed. Section V evaluates the proposed model against the various e-assessment authentication schemes with respect to the impersonation threats and other security issues. Finally, the conclusion is presented in section VI.

II. USER AUTHENTICATION

User authentication is considered the first line of defense in any secure system. It is one of the famous four security requirements; confidentiality, integrity, availability and authenticity [10-14]. These requirements can be implemented in e-learning to ensure that lecturers, students and data are protected against possible risks. User authentication verifies a user's identity whilst trying to access system resources by ensuring who is granted access to which resources [10-14].

Roedunet International Conference (RoEduNet), 2011 10th
Issue Date : 23-25 June 2011 **On page(s):** 1 – 5

A. Authentication Methods

Several methods have been proposed for user authentication. These methods have been divided into three categories called factors, as follows [4]:

1) Knowledge Factors: a user has to know something unique (e.g. a password) that others do not know. This password may consist of a combination of characters, numbers and/or symbols. With a strong password policy, unauthorized parties cannot access others accounts.

2) Ownership Factors: a user should possess a token that others do not, such as a dongle, a key or a card. Unauthorized parties cannot access users' information unless they obtain this token.

3) Inherence Factors: provide accurate means of authentication, but expensive and difficult to implement. Two main methods have been implemented [4]:

a) Something the user is: based on unique features of a user such as fingerprint, voiceprint, retinal pattern and DNA, it provide reliable user authentication.

b) Something a user does: based on unique features of doing things such as handwriting, walking gait and keystroke dynamics, it provides efficient continuous authentication.

B. Continuous Authentication

More cautious should be taken in online examination, where e-learning systems should verify that an examinee is the actual student throughout his exam [1-7]. Multiple technologies and tools are supposed to provide cheating-free e-examinations [1, 6]. Continuous random authentication has been proposed for this purpose [3-7]. It has been shown that confidentiality, integrity and availability (C-I-A) security goals protect e-assessment hardware, software and data against interception, modification, interruption and fabrication threats [7]. However, C-I-A security goals alone are not enough for e-assessment authentication. Hence, different goals are required in order to ensure continuous protection [6, 7]. Three goals have been proposed for this purpose as indicated in Fig. 1 [6, 7]:

- Presence and continuously authenticated presence (specify examinee's place).
- Identity (differentiate an examinee from another).
- Authentication (prove examinee's claimed identity).

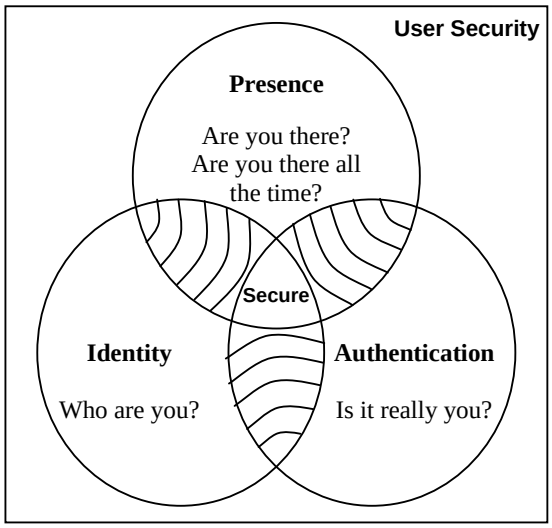

Figure 1. Presence, identity and authentication in e-assessment [7].

C. Drawbacks

Although some of the authentication methods (factors) are highly reliable, they all have some drawbacks when used in e-examination, as illustrated in Table I. In fact, even the most accurate schemes are still vulnerable to several risks. For instance, four risks have been identified in biometrics authentication approaches [6]: (1) fake input, (2) low-quality input, (3) biometric-database modification, and (4) feature-extractor modification. Several methods have been proposed to protect different systems against these risks [6].

TABLE I. DRAWBACKS OF USER AUTHENTICATION METHODS.

Methods or Factors	Drawbacks
Knowledge factors	• If the password is disclosed, the password security policy will be cancelled even if strong enough [4]. • Requested once at login, saved and repeated by cookies; never trusted for continuous authentication during e-examination.
Ownership factors	• If the token is passed to others, the authentication scheme will be circumvented [4]. • Requested once at login and repeats by cookies; cannot be trusted for continuous authentication throughout e-examination.
Inherence factors	• Accurate means of authentication but requires special-purpose hardware. • Difficult to implement and unreasonably intrusive and expensive [4]. • Not fully trusted, although some approaches repeat authentication randomly throughout e-examination [4, 15]. • Never trusted in case of getting assistance from others.

Compared with the illustrated factors, it will be shown that the proposed model is highly reliable and secure, but requires special-purpose hardware and human intrusion. Also, in the near future, it will be inexpensive, simple and relatively easy to be implemented.

III. E-ASSESSMENT AUTHENTICATION SCHEMES

Several approaches of e-assessment authentication have been proposed in the literature. They provide solutions to the various impersonation threats in e-examinations [4, 6, 7, 15].

A. Authentication Schemes

e-Assessment authentication approaches have been categorized into five main schemes, as follows [4, 6, 7, 15]:

1) Proctored-only: considers traditional in-classroom proctoring the most efficient method. It requires a proctor to monitor the exam-takers during their examinations.

2) Uni-modal Biometrics: employs a single biometrics approach, such as fingerprint, keystroke dynamics, mouse dynamics or handwriting.

3) Bimodal Biometrics: two biometrics approaches are combined to provide user authentication. For instance, fingerprint can be combined with mouse dynamics or with head-geometry detection.

4) Video Monitoring: refers to watching the actions of exam-takers either live or recorded by a proctor during online examinations. A password is required for login.

5) Biometrics and Webcam Monitoring: combines fingerprint and real-time video-monitoring.

B. Impersonation Threats

Impersonation threats in e-assessment are the most vital risks (i.e. cheating scenarios) that might be encountered during an e-exam. They occur when an examinee pretends to be another. They have been divided into three types [7]:

1) Type A: impersonation might occur in two cases: (1) the proctor could not detect it, or (2) he allowed impersonation by force, sympathy or bribery.

2) Type B: occurs when a student passes his security information to another, who uses them to answer the exam on his behalf. Username-password pairs fall in this type.

3) Type C: occurs when a student just login to an exam, letting another to continue on his behalf. Non-shareable attributes such as biometrics fall in this type.

IV. INTERACTIVE AND SECURE ELECTRONIC EXAMINATION UNIT (ISEEU)

A prototype secure unit is implemented on Moodle using PHP, MySQL, HTML, and other scripting languages. This unit is called Interactive and Secure E-Examination Unit (ISEEU). A media server is used for streaming and recording exam sessions to the concerned proctor. The proposed model (i.e. ISEEU) is one of the simplest and the most efficient approaches of authentication in e-exams, where an examinee himself, rather than part of his organs, will be under control continuously throughout his exam. Security and reliability wise, it is proved within this context that it can be more efficient than a traditional approach (i.e. in-classroom sessions).

In this paper, tow structures of ISEEU have been proposed. The first uses a webcam to broadcast exam sessions via a media

server and so is named ISEEU- Web Camera (WC). The second, on the other hand, uses video calls instead, and so is named ISEEU- Video Call (VC). They are both discussed deeply in the following subsections. In both models, a proctor will have multiple video screens, one for each examinee, which can be zoomed in if abnormal actions are suspected. Exam sessions are also recorded in order to be revised in case of uncertainty. Interaction between an examinee and his proctor is achieved through chat, audio, video and special emotions available in a control toolbox.

At the beginning, an examinee logins to the e-learning portal (e.g. Moodle) using his account. When he clicks the "start exam", the exam will be blocked waiting permission, and his webcam starts. After that an examinee will be asked to calibrate audio and video devices. Then his proctor asks him to prove his identity, and the exam can not be started unless the proctor approves it by clicking "approve exam" in the toolbox. When the exam starts, it is locked with a full screen so as to prevent an examinee from access to resources on his computer.

During an exam, a proctor might pause a session, resume it, and generate alerts. The alerts are weighted and appear on a cheating indicator bar that ranges from 0 to 100. The exam will be automatically (or manually by the proctor) terminated at any point if an examinee's violations exceed a specific rate. This percentage can be calculated based on the number of warnings and alarms based on violations issued by the proctor.

A. ISEEU Using a Web Camera (ISEEU-WC)

In this model, an examinee should be connected to a media server (MS) through the Internet via a webcam attached to his terminal (ET), as shown in Fig. 2. The MS, in turn, creates a channel ch_n for each examinee to broadcast the exam session to his proctor through the portal of an e-learning server (ELS). Each examinee's session will be streamed through his channel, and all the video streams appear on the proctor's terminal (PT).

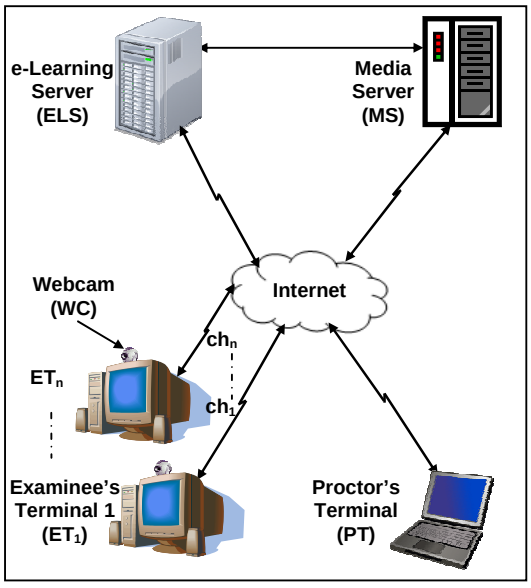

Figure 2. Structure of ISEEU model using a Web camera.

Fig. 3 illustrates the algorithm of the ISEEU-WC. In the 1st step, a student (i.e. examinee) logs in to the ELS, where his identity is initially validated by his username and password. Then, when he tries to start an exam in step 2, the system determines the proctor of his session by querying the database on the ELS (i.e. Moodle), checks whether he is online and notifies him. Step 3 initializes his video/audio devices (e.g. webcam and headphones) and asks him to calibrate them. Then, in step 4, the MS is initialized to start session broadcasting. Step 5 initializes the control toolbox for both examinee and proctor and activates the required functions.

```
1  validateExaminee();
2  findAndNotifyProctor();
3  initVidAudDev();
4  initStreaming();
5  initControlToolbox();
6  Set permitted FALSE;
7  While (takerReady() AND !permitted)
       startDirections();
       if (proctorReady())
           if (takerIdentified())
                   Set permitted TRUE;
                   activateAllToolbox();
8  initTimers();
9  startRecording();
10 startExam();
11 lockFullScreen();
12 While (!timeOver() OR !submit() OR !terminate())
       if (camIsOff())
           pauseExam();
           restartCam();
           resumeExam();
       if (disconnected())
           pauseExam();
           reconnect();
           resumeExam();
       if (procPaused())
           pauseExam();
           if (procResume())
              resumeExam();
13 terminateExam();
14 unlockFullScreen();
15 camOff();
16 stopStreaming ();
17 stopAndSaveRecording();
18 reviewRecAndSubSessionReport();
```

Figure 3. ISEEU algorithm using a Webcam.

Step 6 sets a Boolean value "permitted" to 0, which indicates the examinee is still not permitted to start. He waits in step 7 until his proctor permits him to start the exam. While

waiting, an examinee should play a demo of exam directions and instructions. When the proctor becomes ready, he interacts with the examinee using his toolbox, which contains chat, video, and audio. He follows a predefined procedure to ensure that the examinee is the correct person. If the examinee is identified, the proctor issues permission by setting "permitted" to 1, and all necessary functions of the toolbox are activated.

In steps 8-11, the timers are initialized, the session recording starts, and the exam starts in a locked full screen. The exam session continues in step 12 as well as the examination time is not over, the examinee does not submit, or the proctor does not terminate it. In case of interrupt by some event, such as device failures, disconnection or pause, the system resolves the cause of the interrupt and resumes.

If the proctor terminates the exam for some reason, examination time is over, or the examinee submits his exam, steps 13-17 go as follows respectively; the exam terminates, the full screen is unlocked, the webcam turns off, broadcasting stops, and recording is stopped and archived for further revision in uncertainty cases. Finally, in step 18, the proctor revises the recorded session, if necessary, and submits his final report. This report includes violations and cheating cases, and submitted to the administration for decision making.

B. ISEEU Using Video Calls (ISEEU-VC)

In the previous model, the examinee's computer should be equipped with a webcam and headphones that many students may not have. However, most of students have mobile phones with a built-in camera. The third generation (3G) mobile systems provide customers with video calls service. ISEEU-VC, as illustrated in Fig. 4 utilizes this service to broadcast the exam sessions via mobile phones.

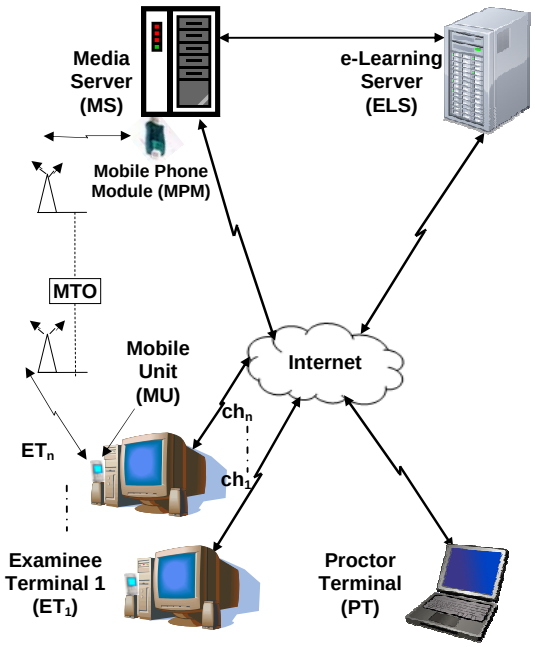

Figure 4. Structure of ISEEU model using video calls.

The numbers of all students' mobiles should be saved in their profiles on the e-learning server (ELS), and a mobile phone module (MPM) will be installed on the media server (MS) through a USB connector. When an examinee tries to start his e-exam, the ELS instructs the MS to place a video call to his mobile. The examinee should accept the call and fix his mobile unit (MU) on its stand opposite to his face. Then the MS starts streaming the video call to his proctor.

The algorithm of ISEEU-WC can be modified slightly to describe the operation of ISEEU-VC. Steps 1 and 2 are not changed, but in step 3, initVidAudDev() method is replaced with videoCall(), which places a video call to an examinee's mobiles. Again, steps 4-11 are not changed. In step 12, the camIsOff() condition is omitted, and the disconnected() condition is replaced with callDisconnected(), which returns 1 when a video call accidentally disconnects. Steps 13 and 14 are not changed. In step 15, camOff() is replaced with terminateCall() that terminates the video call when the exam is submitted or terminated. Finally, steps 16-18 are not changed.

V. EVALUATION

Compared with the previous five schemes, the proposed model (ISEEU) has been evaluated in terms of vulnerability to the different types of impersonation threats and other cheating scenarios. The first scheme is only vulnerable to Type A threats [7], knowing that this scheme is not suitable for e-examinations. The second prevents cheating scenarios of pretending to be the real examinee, hence, solves Type B. It will be suitable for Type C if continuous authentication is performed throughout the e-examination period [7]. In the third, when fingerprint is combined with mouse dynamics, it solves Type B, but unclearly solves Type C due to delay incurred in data-capturing. Alternatively, fingerprint with face-geometry detection offer a promising combination that solves Type B and Type C threats [7]. In the fourth scheme, live video monitoring might fail if the proctor overlooked or unfocussed, while recorded needs extra administrative efforts. It is vulnerable to Type A, B and C threats [7]. Fingerprint of the fifth scheme solves Type B threats, while video monitoring was unclear. Moreover, security will be broken if the view of the webcam is changed [7].

On the other hand, ISEEU is only vulnerable to Type A threats, but vulnerability will be very limited, since a proctor could not allow impersonation for any reason, because all actions are captured and recorded. Institutions might employ monitoring staff who revise all recorded sessions, evaluate them and provide the Administration with comprehensive reports. Moreover, ISEEU efficiently solves Type B and Type C impersonation threats.

In addition, ISEEU resolves several security threats and issues that have neither been resolved nor even mentioned by any of the previous schemes. It solves the following scenarios that the other schemes did not:

- An examinee might look arround at the available resources, such as his textbooks, worksheets, local computer, the Internet and/or get assistance from others. With the continuous monitoring and the full

screen lock function, ISEEU guarantees that all resources including assistance are inaccessible.

- Biometrics schemes, such as keystroke/ mouse dynamics or on-mouse continuous fingerprints, each depends on a specific device that might never or rarely been used while using another device. For instance, an examinee never requires typing in multiple choice questions and rarely requires a mouse in written questions. This scenario is unlikely in ISEEU.
- Finally, the mentioned video monitoring schemes are less efficient, where cheating can not be stopped when detected, since they lack to interaction and cheating indicators. Moreover, the camera might be removed or turned to another object leading to failure. ISEEU provides interaction and cheating indicator bar. Also, an exam will be paused if the camera is turned, moved or removed until being fixed again to resume.

VI. CONCLUSION

It has been shown that e-examination security has been considered a big challenge in e-learning, in which cheating-free e-examination could not be achieved. This paper has proposed a virtual examination unit to resolve this security issue. In this unit a proctor interactively and remotely monitors the examinees throughout their examination. Two models have been proposed for this purpose, and a prototype has been developed on Moodle using PHP, MySQL, HTML and other required scripting languages. Also, a media server has been used for video streaming. Both models operate in the same manner except one difference in the technology of video capturing.

The main advantage of the proposed model (ISEEU) is its efficiency and simplicity. In other words, there is no need for more processing, which is required for image processing and pattern recognition in biometrics methods. It offers exactly the same security or better than in-classroom examination sessions, since it provides the following strength points:

- Full interaction: video, audio, chat, emotions and other functions provided in the control toolbox enable the proctor to interact with the examinees as if they were face-to-face.
- Full security: unlike most of other authentication schemes, there is no way to change or distribute live face and body of an examinee. Also, recorded sessions can be reviewed further in case of impersonation, proctor collusion or uncertainity. More precisely, they provide an evidence of cheating that cannot be denied.
- Psychological factor: the cheating (violation) indicator bar provides an excellent way to make an examinee feels of close monitoring throughout the exam, especially when it increases every time he violates the instructions.

Finally, ISEEU provides a virtual examination environment that supports the C-I-A goals and the three goals of presence, identity and authentication illustrated in Fig. 1. As a result, a cheating-free e-assessment or online e-examination from home will become a reality with ISEEU. Hence, anywhere the proctor is, he can say to his examinees throughout their examinations “look at your screen, I see you”.

REFERENCES

[1] M. Hentea, M. J. Shea, and L. Pennington, “A perspective on fulfilling the expectations of distance education”, Proceedings of the 4th Conference on Information Technology Curriculum (CITC4) Lafayette, Indiana, USA, pp. 160–167, October 2003.

[2] K. Abouchedid, and G. M. Eid, “eLearning challenges in the Arab world: revelations from a case study profile”, Quality Assurance in Education, vol. 12, no. 1, pp .15-27, 2004.

[3] N. H. Mohd Alwi, and I.-S. Fan, M. D. Lytras et al. (Eds.), “Information security threats analysis for e-learning”, Technology Enhanced Learning, Quality of Teaching and Educational Reform, Proceedings of the First International Conference, TECH-EDUCATION, CCIS, vol. 73, Athens, Greece, pp. 285-291, May 2010.

[4] E. Flior, and K. Kowalski, “Continuous biometric user authentication in online examinations”, Seventh International Conference on Information Technology: New Generations (ITNG), Las Vegas, NV, pp .488-492, April 2010.

[5] A. Marcus, J. Raul, R. Ramirez-Velarde, and J. Nolazco-Flores, “Addressing secure assessments for Internet based distance learning still an irresolvable issue”, 9th Latin-American Congress of Educational Computing, Caracas, Venezuela, March 2008.

[6] S. Alotaibi, “Using biometrics authentication via fingerprint recognition in e-exams in e-learning environment”, The 4th Saudi International Conference, The University of Manchester, UK, July 2010.

[7] Kikelomo Maria Apampa, Gary Wills, and David Argles, “User security issues in summative e-assessment security”, International Journal of Digital Society (IJDS), vol. 1, no. 2, June 2010.

[8] Y. Sabbah, “Comprehensive evaluation of e-learning at Al-Quds Open University”, Evaluation Report, Al-Quds Open University (QOU), Open and Distance Learning Center (ODLC), May 2010.

[9] F. Murra, “Current state of e-learning at QOU”, Evaluation Report, Al-Quds Open University (QOU), Measurement and Evaluation Center (MEC), March 2010.

[10] E. Kritzinger, (Eds.) D. Kumar, and J. Turner, “Information security in e-learning environment”, Education for the 21st Century- Impact of ICT and Digital Resources in International Federation for Information Processing (IFIP), vol. 210, pp. 345-349, Springer 2006.

[11] R. Raitman, L. Ngo, and N. Augar, “Security in the online e-learning environment”, Proceedings of the 5th IEEE International Conference on Advanced Learning Technologies (ICALT’05), Kaohsiung, Taiwan, pp. 702-706, July 2005.

[12] W. Stallings, Data and computer communications, 8th Edition, Prentice Hall 2007.

[13] K. El-Khatib, L. Korba, Y. Xu, and G. Yee, “Privacy and security in e-learning”, International Journal of Distance Education, vol. 1, no. 4, pp. 1-19, 2003.

[14] J. F. Gonzalez, M. C. Rodriguez, M. L. Nistal, and L. A. Rifon, “Reverse OAuth: A solution to achieve delegated authorizations in single sign-on e-learning systems”, Computers & Security, vol. 28, no. 8, pp. 843-856, November 2009.

[15] Y. Levy and M. Ramim, “A theoretical approach for biometrics authentication of e-exams”, Chais Conference on Instructional Technologies Research, The Open University of Israel, Raanana, Israel, pp. 93-101, 2007.