1-1-2013

E-Invigilator: A biometric-based supervision system for e-Assessments

Nathan L. Clarke
Edith Cowan University

P Dowland

Steven M. Furnell
Edith Cowan University

e-Invigilator:

A Biometric-Based Supervision System for e-Assessments

N.L Clarke[1,2], P. Dowland[1] & S.M. Furnell[1,2]
[1]Centre for Security, Communications & Network Research (CSCAN), Plymouth University, United Kingdom;
[2]Security Research Institute, Edith Cowan University, Western Australia
e-mail: info@cscan.org

Abstract— **The creation of Virtual Learning Environments (VLEs) have revolutionized the online delivery of learning materials, from traditional lectures slides through to podcasts, blogs and wikis. However, such advances in how we assess such learning have not evolved – with physical attendance at proctored exams still a necessity for formal assessments. This paper presents a novel model to enable remote and electronic invigilation of students during formal assessment. The approach utilizes transparent authentication to provide for a non-intrusive and continuous verification of the candidates identity throughout the examination timeframe. A prototype is developed and a technology evaluation of the platform demonstrates the feasibility of the approach.**

Keywords-e-assessment; e-learning; e-invigilation; biometric

I. INTRODUCTION

E-learning is a widely accepted model for learning with a huge number of providers utilizing platforms to deploy materials and educate students. Within traditional education, e-learning platforms are commonly utilized in conjunction with normal classroom-based education to deploy educational materials and to extend the students knowledge. Moodle, a leading open-source Virtual Learning Environment (VLE) has over 63 million users, 6.7 million courses and 1.2 million teachers [1]. The business case for e-learning seems to suggest that the approach is a "no-brainer", with huge savings possible in teacher time, room costs, travel time and equipment [2].

Whilst much effort has been expended on the creation and deployment of VLEs, less focus has been given to the associated problem of providing e-invigilation. Formal exams and tests still need to be undertaken under controlled conditions within defined classrooms with physical invigilators present to maintain the integrity of the assessment process. This results in a costly model for both the institution and the candidate. Whilst for a subset of students, this is arguably less of a problem, as they are attending class physically, a growing segment of the market is focused upon the complete remote-delivery of courses. In these cases, students that could be studying courses from providers many hundreds of miles away are still required to attend assessment centers to undertake their examinations. The fundamental problem in providing remote assessment is the ability to verify the authenticity of the candidates.

This paper proposes an approach to remote invigilation that seeks to build upon prior research that capitalizes on providing a monitored and supervised environment for the candidate to undertake their assessment through the application of transparent authentication. Current approaches all require a user to intrusively provide an authentication sample (e.g. password or fingerprint); however, in circumstances where the user is complicit in the misuse, such approaches have a significant failing in that users know when and how to circumvent the system. The approach presented in this paper authenticates candidates non-intrusively and continuously throughout their session with the resulting system automatically identifying possible misuse.

The paper begins with an analysis of the current state of the art in e-assessment and goes on to describe the domain of active authentication. Sections 3 and 4 present a model and prototype implementation for achieving e-invigilation. The paper then concludes with a discussion and identifies areas for future research.

II. BACKGROUD RESEARCH

A. E-Assessement

Prior literature into e-Assessments has largely focused upon the desired to increase invigilation and monitoring within a classroom or controlled environment during assessments that utilize computers. They are designed not to replace physical invigilators but to provide additional layers of monitoring to ensure candidates are not performing any actions on the PC that does not confirm to the assessment policy (i.e. using an Internet browser to search for a solution). Many of these systems incorporate some network-based monitoring, which in itself requires appropriate network infrastructure and monitoring software. Percival et al proposed "The Virtual Invigilator", an approach that utilizes Intrusion Detection-type functionality to detect possible deviations away from standard procedure [3]. Other approaches, such as commercial offerings by Software Secure and Respondus have taken the approach of locking down what the browser and/or system is able to do during an assessment, thereby removing the opportunity for possible misuse [4,5]. Yuan and Yang [6] have proposed a SIP-based video surveillance system. Whilst these approaches all have merit and are certainly required within an e-invigilation system, they fundamentally fail to verify the authenticity of the user.

Software Secure have recognized the desire for remote-proctoring of exams; however, their solution incorporates real-time videoing of the candidate during the assessment. Whilst this does provide a level of authenticity, the real-time nature of the capture is storage and bandwidth heavy and the solution still requires a manual inspection by the academic to verify whether any problems exist. No level of automation exists within the process.

The ability to fundamentally verify a user's authenticity has been previously addressed within classroom-based scenarios and a number of commercial partners such as Remote Proctor by Software Secure provide a fingerprint recognition system. The premise of the concept of utilizing biometrics to verify a users' authenticity is certainly stronger than using passwords; however, their implementation to date has two significant drawbacks. Firstly the Remote Proctor system requires dedicated hardware. Whilst feasible within a classroom environment, the idea of requiring each candidate to purchase the hardware for remote assessments is unlikely to be very cost effective. The more significant issue however is with respect the nature of the authentication. In all cases described in the literature thus far, authentication of the user is performed intrusively and thus the user is aware when credentials are required. In an environment where a candidate is looking to cheat, this provides information to the user as to when to provide the sample. Furthermore, beyond the initial verification at the beginning of the assessment, no further verification is performed – although levels of monitoring through video and microphones can be provided.

A system that is capable of authenticating a user non-intrusively or transparently would provide a mechanism for continuously verifying the authenticity of the user but without them having to explicitly provide a credential or biometric sample.

B. Active Authentication

The domain of active authentication is relatively new in comparison to traditional authentication technologies. Its focus is on the ability to non-intrusively and continuously authenticate a user utilizing (largely biometric-based) credentials obtained from the user whilst they normally interact with the electronic device or system. For example, with the context of a mobile device, a number of biometric-based approaches can be utilized to transparently capture and verify the authenticity of the user (as illustrated in Fig. 1).

Figure 1. Transparent Authentication within a Mobile Device

A wide range of literature exists within the domain, with many research studies looking at developing transparent biometric techniques and considering the architectural issues that exist when developing a multimodal biometric system [7,8]. The approach, referred to as TAS – Transparent Authentication System – has a generic architecture that involves the non-intrusive capture of biometric samples, extraction and processing prior to verification and intelligent monitoring (as illustrated in Fig. 2). The types of authentication approaches that lend themselves to non-intrusive authentication do vary in terms of their authentication performance. The stronger biometric techniques such as fingerprint recognition do not lend themselves to transparent capture. It is the weaker behavioral-based approaches that tend to (but not exclusively) contain a non-intrusive component.

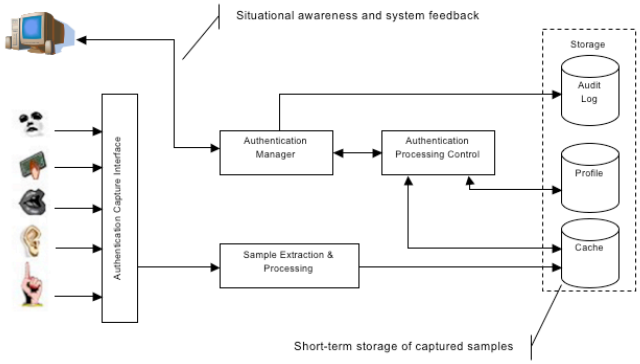

Figure 2. A Generic TAS Framework (Clarke, 2011)

The key advantage of applying a TAS-based approach to e-invigilation is the unpredictable nature of the biometric capture, with samples being taken continuously throughout the assessment without the candidates' knowledge the sample is being taken. The system also provides the capability to automatically perform verification of the candidate through utilizing biometric systems, enabling academics to easily identify possible candidates that have misused the system.

III. A Model for E-Invigilation

The application of TAS to e-invigilation provides a series of distinct advantages over existing approaches:

- It removes the ability for the candidate to authenticate to an exam or provide credentials to do so and subsequently allow another individual to actually take the assessment.
- It provides continuous verification of the user throughout the session.
- It provides the academic with an automated means of identifying misuse through flagging candidates whose biometric samples fail.
- It does not require any specialized hardware or additional biometric capture devices over standardized PC hardware (e.g. keyboard, camera, mouse and microphone).

As illustrated in Fig. 3, the model for e-Invigilator is a flexible and modular framework that permits the inclusion of suite of transparent biometric techniques. Which techniques are in use will be a function of the candidate's hardware (i.e. do they have the necessary biometric capture technology), the academic requirements (i.e. the academic might decide upon a specific suite of techniques to be used), the availability of biometric software (i.e. the system has the backend biometric software to process the samples). It is envisaged that a wide-range of transparent biometric techniques could be suitable within the e-Invigilator, but which techniques are appropriate will depend upon the nature of the assessment. For instance, if the assessment requires oral responses, then voice verification can be utilized. If the assessment requires textual-based inputs then keystroke analysis or linguistic analysis could be appropriate. In the majority of scenarios it is envisaged that facial recognition will be available – as this is a technique that lends itself particularly well given the natural placement of a web camera on top of the laptop or monitor screen.

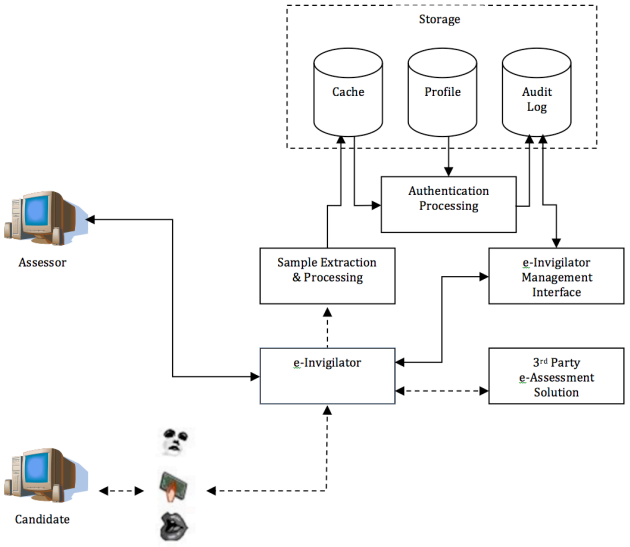

Figure 3. An Architectural Model for e-Invigilation

From a process perspective, e-Invigilator is designed to be lightweight and user friendly. As such the system is deployed via a web browser, removing any need to download and install applications. The system is split into two modes of operation dependent upon the role of the user: candidate (highlighted with a dash in the figure) or assessor (highlighted with a solid line in the figure). The purpose of e-Invigilator is not to provide the e-assessment platform. There are already pre-existing systems that provide a whole host of functionality for supporting numerous assessment types. E-Invigilator is rather an umbrella, which provides for authentication and monitoring of the candidate independent of the e-assessment solution. The only assumption with this solution is that the e-assessment solution can be provided through a web browser.

It should also be noted that although the model in Fig. 3 does not specifically state it, it is assumed that such a system would incorporate the monitoring and lockdown functionality that pre-existing systems have already established. The purpose of this diagram was merely to emphasis the transparent biometric functionality.

As depicted in Fig. 4, the process model presents a process for enrollment and subsequently the ability to undertake assessments for the candidate role. With respect to the assessor role, they have the capability of creating new assessments, adding student cohorts and managing the results of the assessment (from a biometric perspective).

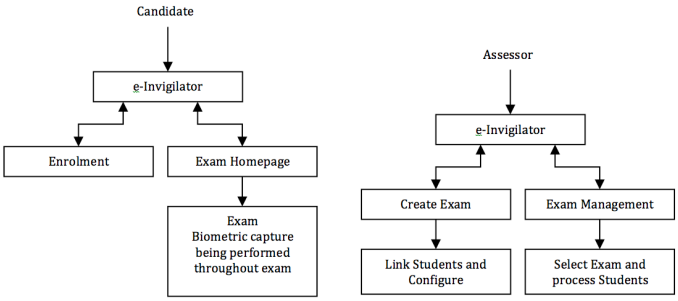

Figure 4. A Process Model for e-Invigilator

IV. Prototype Development of E-Inviglator

A prototype of the aforementioned model was developed in order to better assess (in the first instance) the technological aspects of such a model. Due to financial development costs, the range of biometric technologies supported by the prototype was restricted to facial recognition only. Whilst limiting, it was felt such a restriction would not have an impact on the technology evaluation.

In order to highlight the ease of use and lightweight nature of the model, screenshots of key functionality are provided below. Fig. 5 presents the interface for the assessor to create and define an exam. The start and end timestamps and duration can be utilized to enable the assessor to either restrict candidates from taking an exam until a predefined slot, or alternatively, the assessor can set this up so that the candidate is able to undertake the exam at any point between the two dates. This particular setup of the model has been developed with Plymouth University internal systems in mind, with the ability to directly link a student cohort to the exam (and thus remove the need to enter a list of students that are taking each exam).

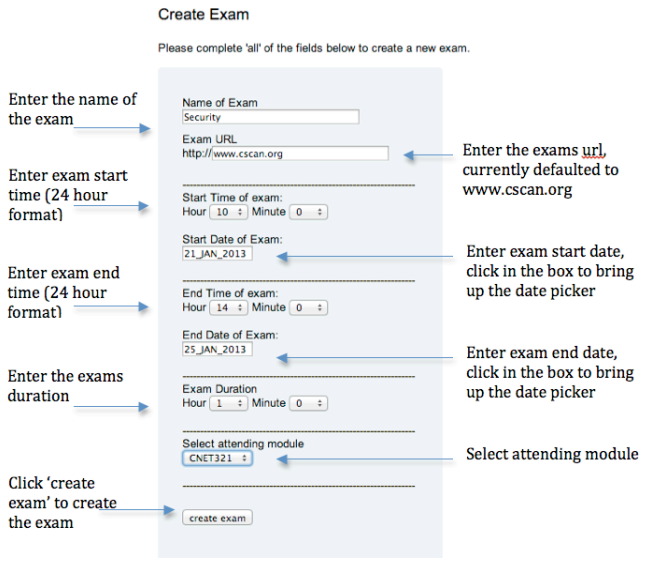

Figure 5. Exam Creation Interface

Assuming an individual assessor has multiple exams setup, the *Exam Management Interface* provides an overview of all current and previous exams that have been defined during any particular academic year. As illustrated in Fig. 6, the system provides a quick and easy approach to identifying which exams have students failing (biometrically) so that the assessor can query that exam.

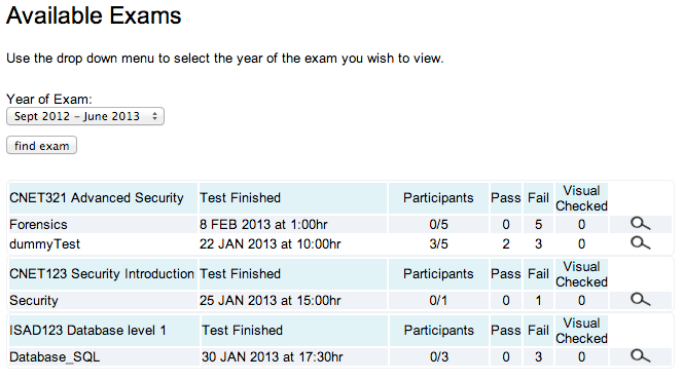

Figure 6. Assessors Exam Management Interface Overview

Clicking on the search icon (in Fig. 6) provides a detailed listing of all candidates assigned to the examination with a traffic-light system indicating which students have undertaken the assessment and whether they have passed or failed the biometric test (as illustrated in Fig. 7). Candidates that require further examination, can be checked through a subsequent interface that provides all candidate biometric information. For techniques, such as face and voice, these samples provide the assessor with a further manual verification if required. Samples marked in red are those that have failed the biometric test. Please note, for privacy purposes the image shown in Fig. 8 is a mockup of the functionality rather than an actual person's face.

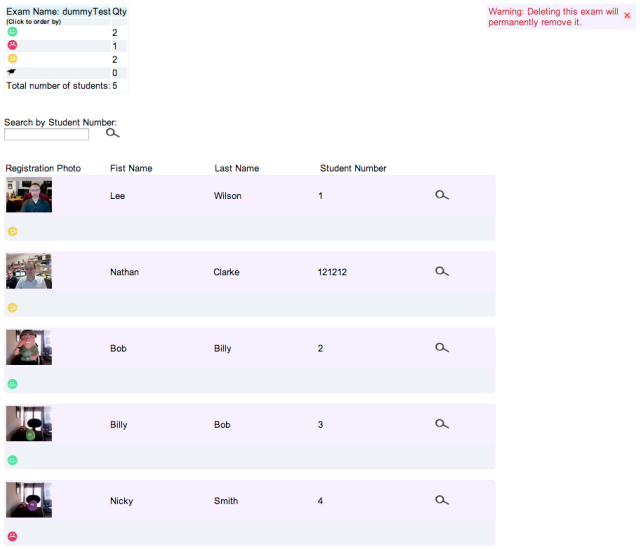

Figure 7. Assessors Individual Assessment Interface

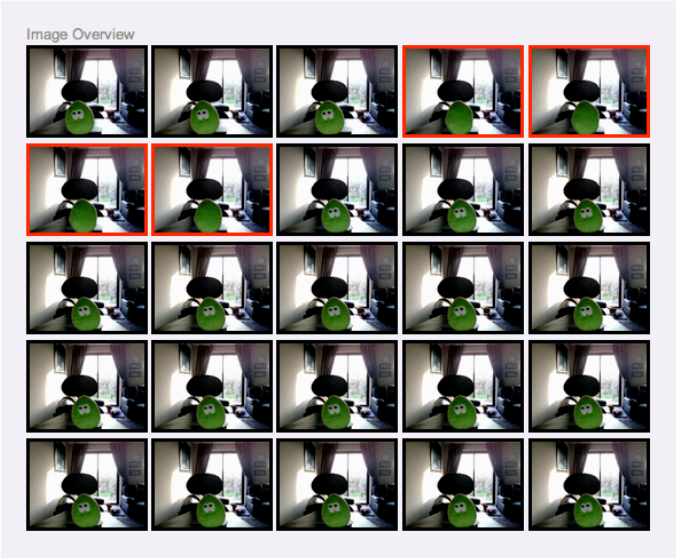

Figure 8. Figure 8: Assessors Individual Candidates Interface

The student's view of the software has been kept very simplistic. The authentication credentials required to initially login to the system are based upon their wider Institutional credentials using delegated authentication. Upon login, the candidate is initially provided with a screen for enrolment – in this case, the system takes a series of images of the user, which are subsequently used in verification phase. After enrolment has been completed, the candidate will be presented with a screen listing the available assessments for them. Clicking on the assessment will result in the third party e-assessment loading. From an e-invigilation perspective, a small window in the upper right hand side of the browser presents a video of the camera taking the facial recognition. Whilst no indication is provided to the candidate about when an image is taken, the purpose of this screen is to provide feedback to the candidate that the e-Invigilation software is in operation.

V. DISCUSSION

The use of biometric technologies that require no additional hardware and are transparent in nature clearly has a distinct advantage over pre-existing solutions. There are however, a number of aspects that require further consideration.

For instance, whilst the prototype demonstrated the capability of acquiring image samples from within a web browser and successfully uploading the images to the e-Invigilation servers with no impact on the candidates ability to undertaken the assessment through the third-party provider, concerns do exist over the scalability of such a solution – both in terms of the individual system capturing and processing multiple biometric samples and also in terms of how many concurrent users would a server be able to cope with. The "umbrella" nature of e-Invigilator has specifically been designed not to present any impact upon the candidate or the third-party e-assessment tool. For it to do so could have an impact upon the candidate's ability to perform.

The prototype has been designed specifically with facial recognition in mind, as it is an approach that can be tested both automatically through biometrics but also manually verified if required by the assessor. Not all biometric technologies would enable such manual assessment and therefore the performance of the underlying biometric becomes even more important. With facial recognition it is less important if the biometric flags misuse when none is present, as the assessor can manually check. This has implications over how each biometric technique is setup and configured in terms of the performance it is trying to achieve (i.e. a threshold, which is essentially a measure of similarity between the enrolment and verification samples, needs to be set). For face, due to the availability of manual checking can have a value set that is on the cautious side. However, for other approaches, such as keystroke analysis or linguistic profiling, with no manual verification possible, the technique needs to be strengthened.

The final aspect that needs to be highlighted is the current availability of transparent biometric technologies. Whilst biometrics themselves have proven increasingly popular, their success is largely dependent upon their application in very controlled environments. With transparent approaches, they have an inherent requirement to operate in less controlled environments and as such it is not advisable in most cases to directly deploy an intrusive biometric technique in a non-intrusive manner. As such, few transparent authentication techniques currently exist commercially. That said, research into the development of transparent biometrics has been on going for a number of years and it is envisaged that such techniques will be available in the future [9, 10, 11, 12].

VI. CONCLUSIONS & FUTURE WORK

The paper has proposed an approach to provide remote-based e-Invigilation of assessments through the use of transparent biometrics. This removes the need to have physical invigilators, assigned classrooms or assessment centers and provides both the assessor and candidate with a degree of freedom yet providing the level of integrity you would expect from a formal assessment procedure.

Whilst the prototype has undergone a technical evaluation to determine whether such a model is feasible, further validation of the model under stress is required. Future work will therefore focus upon performing a full evaluation of the software with a group of candidates undertaking an assessment concurrently. The evaluation will also include an end-user survey to ensure no negative impact upon the assessment process is experienced and to measure the overall usability of the system.

REFERENCES

[1] Wikipedia. Moodle. http://en.wikipedia.org/wiki/Moodle (Accessed: 25 Feb 2013)

[2] Kineo. Tip 7: Making the case of e-learning. http://www.kineo.com/elearning-tips/tip-7-making-the-business-case-for-e-learning.html (Accessed: 25 Feb 2013)

[3] Percival, N., Percival, J., Martins, C. The Virtual Invigilator: A Network-based Security System for Technology-Enhanced Assessments. Proceedings of the World Congress on Engineering and Computer Science, San Francisco, USA, October 22-24, 2008.

[4] Software Secure. Remote Proctor. http://www.softwaresecure.com/solutions/remote-proctor.html (Accessed: 25 Feb 2013)

[5] Respondus. Respondus – Assessment Tools for Learning Systems. http://www.respondus.com/ (Accessed: 25 Feb 2013)

[6] Yuan, C., Yang Q. "The Scheme of SIP-based Video Surveillance System". Second International Workshop on Education Technology and Computer Science, vol. 3, pp. 268-271, 2010.

[7] Clarke NL. Transparent Authentication. Springer. ISBN: 978-0-85729-804-1, 2011.

[8] Clarke NL, Furnell SM. "Advanced user authentication for mobile devices". Computers & Security, 2007.

[9] Clarke NL, Furnell SM. "Authenticating Mobile Phone Users Using Keystroke Analysis". International Journal of Information Security, vol. 6, no. 1, pp1-14, 2006.

[10] Clarke NL, Karatzouni S, Furnell SM. Transparent Facial Recognition for Mobile Devices. Proceedings of the 7th Security Conference, Las Vegas, USA, 2nd-3rd June, 2008.

[11] Clarke, NL, Mekala, AR. "The application of signature recognition to transparent handwriting verification for mobile devices". Information Management & Computer Security, vol.15, issue. 3, pp.214-225, 2007.

[12] Traore, I., Ahmed, A. Continuous Authentication using Biometrics. IGI Global. ISBN: 978 1613501290, 2012.