

Keeping the wolves from the doors... wolves in sheep's clothing, that is

Robert Fröhlich
Division of Electronic & Broadcast Media,
Nanyang Technological University, Singapore
email: tfrohlich@ntu.edu.sg
telephone: +65 790 6453
fax: +65 792 7526

Abstract

In traditional face-to-face environments, we have been able to confirm the identity of students who are undertaking assessment. We have also been able to ensure the security of the exam papers and scripts during examination processes, including the transportation to and from the exam hall. These security issues have been moved into a state of flux with the use of flexible delivery methods. Students may now be scattered from one side of the globe to the other. Is it realistic to require foreign students to attend examinations at the Institution originating the course, or even to attend authorised examination centres within their country of residence? Is it even feasible to establish authorised examination centres at all locations where students may possibly study? With computer assisted assessment, conducted on-line, it is now possible for students to participate in assessment tasks and examinations from any location on the planet. However, how do we authenticate and invigilate these assessment processes? Is it the actual candidate, sitting the exam or participating in the assessment? How can we ensure that the person sitting at the computer is in fact the intended student?

This paper examines the emerging new media communication hybrid technologies and devices, including authentication and cryptographic technologies, and highlights how these may be effective for the facilitation of Authenticated Secure On-line Computer Assisted Assessment (ASOCAA). These authentication and security methods will empower educators to construct more flexible assessment environments, where all participants (both faculty and students), can be assured that the assessment process is secure and authentic. This in turn will provide a richer learning experience for students undertaking flexible and distance learning.

Keywords

Cryptography, Biometrics, Identification, Authentication, Security, Invigilation.

Introduction

We are all familiar with the typical examination situation: the candidates swell through the examination venue doors looking for their assigned location within the venue; are advised by a Chief Invigilator that they may not turn-over their exam papers and commence reading until the exam has commenced; are reminded of the requirements of the examination session including the advice as to what materials may be present in the venue and that pagers and mobile telephones should be handed in to the invigilators or left outside; that their identification cards are to be placed on the desk in front of them so that the invigilators can check their identity during the exam; that they should only write on the ruled pages within the examination answer booklets and do any rough work on the un-ruled pages which will not be marked by the Examiner; and that no materials may be removed from the examination venue at the conclusion of the examination, other than the examination question papers.

Once the examination has commenced, the invigilators make their way around the venue and check that each candidate's face resembles the face that is shown on the respective identification card. Often the photo is that old that it is indeterminable as to whether the candidate is in fact the correct person, as the hairstyle and maturity of the individual may have changed dramatically since the it was taken. Another hindrance, is the fact that the candidates are usually deeply engrossed in thought and writing furiously, so that they can answer all the required questions in the available time, and so have their heads buried in their work and are not as such in a position which readily facilitates identification by the invigilators. One saving grace, is that the examiner can often recognise the students who have participated in the classes and so believes them to be valid candidates, although it has been known for enterprising students to arrange for a competent imposter to take a whole course on their behalf.

This traditional formal assessment process has no guarantee for confirmation of the identity of the candidates undertaking the examination and although it is usually successful, has inherent authentication problems. How can we be confident that the examination candidate is indeed whom they are supposed to be? In the delivery of examinations for distance candidates, the authentication process can be even harder. It is unlikely that the Invigilator will always be able to categorically identify all candidates by the likenesses shown on their identification cards, even when this process is substantiated by other forms of identification.

Employing New Technologies

There are various New Media Communication Hybrid Technologies and devices, which may lead to educators being able to offer on-line examination environments with enhanced security. Various combinations of these systems need to be employed by institutions and educational bodies if they wish to offer Authenticated Secure On-line Computer Assisted Assessment (ASOCCA). Credibility of web-based assessments and on-line assessments can only be assured once we can substantiate the identity of the participants and assure the security of the assessment process. In this situation, security involves both the confirmation that the assessment has not been tampered with throughout the process of transmission, in both directions, and that the participant has not had any unauthorised assistance to complete the assessment tasks.

Security

The first factor necessary for securing web-based and on-line assessments, is ensuring that the data transmitted is not tampered or interfered with whilst it travels both from, and to, the assessing organisation. This security can be provided by a combination of secret and public key cryptography. In secret key or symmetric cryptography, "the sender and receiver of a message know and use the same secret key: the sender uses the secret key to encrypt the message, and the receiver uses the same secret key to decrypt the message. In public key cryptography systems, each person gets a pair of keys, one called the public key and the other called the private key. The public key is published, while the private key is kept secret. The need for the sender and receiver to share secret information is eliminated; all communications involve only public keys, and no private key is ever transmitted or shared. Anyone can send a confidential message by just using public information, but the message can only be decrypted with a private key, which is in the sole possession of the intended recipient" (RSA Security Inc., 1999). These public key cryptography systems are available from many sources including RSA Security Inc., CyberGuard Corporation and others. For ASOCCA, an additional layer of secret key cryptography can be overlayed, with the additional key taking the form of electronic passwords which are derived from data provided through a matrix created by the biometric identification systems described later in this paper.

The second factor, the invigilation process, may in fact be the most difficult part in providing ASOCCA. Even in traditional examination halls, with human invigilators, it is nearly impossible to confirm that students do not have assistance throughout the examination by way of devices such as covert security kits. These kits provide a wireless earphone, where a miniature radio receiver is housed in what would appear to be an in-ear hearing aid, and a transmitter for the facilitation of two-way communication is concealed in a pocket. The only way

to categorically determine that such devices are not used would be to fully search examinees upon their entry to the examination hall. Current metal scanning technologies would appear to be ineffective for this function, due to the miniature size of these devices. One way of possibly detecting the use of this type of device, would be to scan all of the radio frequency bands within the examination venue and then determine the content and origin of any broadcast received. Another may be to totally shield the examination halls from radio frequencies by way of a faraday shield. Such a shield would need to be built into the structure of the examination venue upon its initial construction, as retrofitting would prove difficult. Both of these methods of detecting the use of covert radio devices would surely prove impractical for even well funded institutions.

Biometric Identification and Authentication

It appears that with existing technology, though most biometric products boast very high success rates using only one system, failsafe authentication may only be provided through a combination of two or more biometric systems. Biometric systems can be defined as "automated methods of verifying or recognizing the identity of a living person based on a physiological or behaviour characteristic" (Miller, 1994). In simple terms, they are computer systems that can authenticate the identity of the individual who is using them. These systems currently make use of the difference in the individual characteristics within a persons fingerprint, hand geometry, iris, retina, face, voice, or handwriting. In the future, biometric systems may even utilise DNA to facilitate identification. Microsoft has recently announced that later this year it plans to embed biometric identification techniques similar to these into its Windows™ operating systems (Microsoft, 2000).

Fingerprint Recognition

Fingerprint -based identification is one of the oldest methods of identification and has been successfully used in numerous biometric applications (Michigan State University). Currently fingerprint reading technology utilising minutiae techniques (where a matrix is constructed of the points of a fingerprint where the ridges join or split), is currently available for under US\$170 (Veridicom, 2000). This matrix, created from a scan of the users fingerprint, can be in the form of a file smaller than 300 bytes. This can be easily stored on a smart card. To facilitate identification or authentication, the user simply places their finger on a small fingerprint reader, which either utilises optical scanning or thermal scanning (Neurodynamics, 2000a), and the program then recreates the matrix from the scanned fingerprint. The resultant matrix file is then either matched with a record from a database (in order to identify and authenticate the user), or may be matched to a single portable secure record, such as that stored on the smart

card (in order to facilitate authentication only).

Smart Cards

Smart card reader/writers are available for under US\$150 (Innovonics, 2000), and the current generation of smart cards have a storage capacity of up to 32 Kilobytes (Smart Card Basics, 1999). Combined with the fact that smart cards are a relatively cost effective form of visual identification (incorporating a photo of the user), they are also an optimum system for providing portability of a user's enrolment data. This data is recorded in the form of a secure file that is stored on the smart card. This portability means that the delivery site need not be connected to a large database in order to identify the user, as the user's identity can be derived for the file stored on the card. The biometric system merely authenticates the user based on the data stored on the card. Smart cards are in the process of being piloted in the city of Southampton, in the UK, as a form of identification for all residents. The pilot, utilising smart cards for transportation, entertainment, education and other services in this English city of 215,000 citizens, is co-funded by the European Commission and will conclude in November, 2002 (Smart Card Central, 2000).

Hand Geometry

Hand geometry recognition systems are already employed in the dining facilities, residential housing and the new, state-of-the-art recreational facility at the University of Georgia (Recognition Systems Inc., 2000). These systems utilise biometric technology that identifies people by the size and shape of their hand.

Retinal Scans

Retinal scans have been commercially used as a form of identification since 1985 (Dysart, 1998). They utilise the patterns created by the blood vessels on the back of the user's retina. Retinal scans usually require that the user place their head in a positioning support, while a low powered infra-red light is focussed on their retina in order to derive an image of the retina. Because of this relatively invasive process, they are not favoured as an efficient biometric technique.

Iris Recognition

A newer method of accurate identification is through iris recognition. Individual's iris characteristics change very little over the duration of their life. These characteristics enable a biometric system to produce a matrix, where a series of

concentric circular zones are established, and the textural information (lightness and darkness of the image) along the circumference of each zone is extracted (Dysart, 1998). Iris recognition technology utilises a special camera to capture an image of the user's iris. This image is then compared with pre-enrolled images either stored on a database, or on a smart card. Systems utilising this technology are available for less than US\$300 (Iriscan Inc., 2000; Sensor Inc., 2000; Visionics, 2000), although some of these systems cost up to US\$50 to enrol each user.

Facial Recognition

Traditional two-dimensional biometric facial recognition is achieved through analysing measurements of angles and distances between broad facial features such as the eyes, nose and mouth. Full three-dimensional biometric facial recognition utilises neural networks to generate a true three-dimensional representation of the subject's face, so that more subtle features such as the bone structure around the eyes and nose can be analysed (Neurodynamics, 2000b). This three-dimensional approach provides more accuracy in recognition, even when there are facial changes, such as the subject wearing glasses or growing a beard.

Voice recognition

Voice recognition is already employed in the operating system of Apple Macintosh[™] computers (Mac OS 9) through a system called voiceprint. Because no two individuals vocal tract dimensions, acoustics and excitation are alike; no two voices are alike. Therefore, it is believed that no two voiceprints are alike and an individual's voiceprint is as unique as a fingerprint. This biometric technology, in the form of the "Star Trek Voice Print Verification PC Security Software" produced by QVoice Inc., is available for Windows[™] systems for less than US\$80 from the LoneZone[®].

Remote Invigilation

In order to be able to successfully invigilate remote assessment locations, it is important to be able to view all occurrences at the location. This may be facilitated with devices such as the Omnicamera, which was developed at Columbia University and is marketed by RemoteReality as the ParaCamera[™]. Essentially the Omnicamera is a video camera that can view in all directions simultaneously. Using parabolic optics, the camera provides a 360° x 180° image which when decoded, through the Omnivideo software (ParaPlayer[™] software), produces images of normal perspective at full video frame rate.

Viewers can select any perspective or viewing direction and magnification from the video signal containing the full 360° x 180° image. This technology can allow remote invigilators to navigate (pan, tilt and zoom) within both live streaming video environments and recorded video footage from the examination location. Full omnidirectional video imaging is possible through a combination of two Omnicamera sensing units mounted back-to-back, although if one Omnicamera is located on the ceiling of the examination location, this may be unnecessary.

ASOCCA in Practice

The reliability of the technologies examined in this paper is increasing as time goes on. There are also competing technologies, in many of the fields described, developing at a blinding rate. It appears therefore, that there are few barriers to offering ASOCCA in the field. Most of the technological solutions and components required to create such a system are already available commercially, and for relatively low cost. It is merely a matter of integrating these components into stand-alone systems, which are not cost prohibitive for both the assessing organisations and their remote participants.

References

- CyberGuard Corporation (2000) *CyberGuard Corporation - Firewall - VPN - Encryption - High Availability Solutions* <<http://www.cyberguard.com/>> (8 May 2000).
- Dysart, A. (1998) *Biometrics Paper* <<http://www.monkey.org/~adysart/598/>> (8 May 2000).
- Innovonics. (2000) *Innovonics PC Pay® developer kit Online Order Page* <<http://www.innovonics.com/pcpay/purchasing/purchasing.html>> (8 May 2000).
- Iriscan Inc. (2000) *Iris Recognition Products* <<http://www.iriscan.com/html/irisrecogproduct.html>> (8 May 2000).
- Michigan State University, Department of Computer Science and Engineering, Pattern Recognition and Image Processing Lab. *Biometrics:Fingerprint* <<http://biometrics.cse.msu.edu/fingerprint.html>> (8 May 2000).
- Microsoft Corp. (2000) *Microsoft and I/O Software Strengthen Industry Adoption of Biometrics* <<http://www.microsoft.com/PressPass/press/2000/May00/BiometricsPR.asp>> (8 May 2000).
- Miller, B. (1994) "Vital Signs of Identity". IEEE Spectrum 22-30.

Neurodynamics Limited. (2000a) *DSX1 - A single chip, thermal fingerprint sensor* <http://www.neurodynamics.com/Biometrics/Biometrics_PDFs/Dxs1.pdf> (8 May 2000).

Neurodynamics Limited. (2000b) *NVisage - Adding a new dimension to facial recognition* <http://www.neurodynamics.com/Biometrics/Biometrics_PDFs/NVISAGESHEET1.pdf> (8 May 2000).

QVoice Inc. (1999) *QVoice Inc.* <<http://www.qvbiometrics.com/>> (8 May 2000).

Recognition Systems Inc. (2000) *About Recognition Systems - Biometrics, Hand Geometry, Access Control, Time & Attendance, Personal Identification, Security* <http://www.recogsys.com/rsi_public_html/about.html> (8 May 2000).

RSA Security Inc. (1999) *RSA Laboratories FAQ 4.0 - Frequently asked questions about today's cryptography* <<ftp://ftp.rsasecurity.com/pub/labsfaq/labsfaq4.pdf>> (8 May 2000).

Sensar Inc. (2000) *Sensar's Online Demonstration* <<http://www.sensar.com/demo/demo.htm>> (8 May 2000).

Smart Card Basics.Com. (1999) *Smart Cards and Security Overview* <http://www.smartcardcentral.com/news/pressrelease/schlumberger_041300.asp> (8 May 2000).

Smart Card Central (2000) *Smart Card Central News* <http://www.smartcardcentral.com/news/pressrelease/schlumberger_041300.asp> (8 May 2000).

The LoneZone® (1999) *Star Trek Voice Print Verification PC Security Software* <http://www.lonezone.com/MIND/SECURE/8828_z7.html> (8 May 2000).

Veridicom (1997-2000) *Product Overview* <<http://www.veridicom.com/products/overview.htm>> (8 May 2000).

Visionics (2000) *Visionics Corp. - Makers of FaceIT®* <<http://www.visionics.com/>> (8 May 2000).