Practical application of biometrics for security, privacy and convenience within the UK education environment

Aine Ni Fhloinn
Inhouse Training
32 Northbrook ave.
Ranelagh, Dublin 6, Ireland
E-mail: info@inhousetraining.ie
www.inhousetraining.ie

Abstract: *This paper reports on identification needs within a UK secondary school environment. The motivation behind the final biometric enabled system choice is discussed and a system design is presented. How the system will operate is portrayed using a typical school day for user groups (Students, Teachers, Administration and Parents). As enrollment for the system is non-mandatory, privacy concerns for user groups influence acceptability of the system. The paper discusses legal protections which help form the parameters of the system design and recommends further management policies that will enhance usability for each user group.*

Key words: identification, biometrics, privacy, policies, Data Protection Act.

1. Introduction

This paper presents identification problems for a secondary school environment and a system design which incorporates a biometrically enabled identification system, a school management platform and management policies. The paper is based on a pilot project currently planned for implementation in a South of England secondary schools. The goal of the project is to solve identification concerns as experienced by students, teachers, parents and administration staff. The system design is not required to provide for physical security (such as gates/doors) but to act to support identification needs for the school. Participation in the system is non-mandatory for all user groups. This has the effect of security mechanisms performing to support privacy expectations of user groups.

To begin with, identification problems for each user group are clarified together with a description of the current system response. Motivation for selecting a school management system that incorporates iris recognition technology and RFID is then presented. The impact of the proposed system design is explored in terms of a typical school day for each user group (students, teachers, parents and administrators). Usability of the system is dependent on trust in security and policies that act to support privacy. This paper discusses legal obligations and concludes with recommendations on management policies for the planned system.

2. Identification problems within a secondary school environment (UK based) according to user group (Administration, Students, Teachers, Parents)

For secondary schools, school administration staff more often than not cover security as part of administration duties. But for the sake of clarity, these duties are segregated into security and support under the same heading of Administration.

2.1 Administration Perspective

Security - Problems Area (regarding identification needs)

There is an inability to make use of staff/student vigilance regarding strangers on property. Vandalism (lack of ability to pinpoint witnesses or perpetrators) is an increasing problem. Poor personal security management on the part of regular staff/students is also increasing i.e. swapping/losing/forgetting swipe cards.

When new staff/students are not recognisable by peers, it potentially allows intruders to freely mingle. Changes in physical appearance of students over time adds to this difficulty. A lack of communication facilities will underline this.

Break ins (deciding if problem is internal involving collusion) and false alarms are also identification issues.

Administrative Support - Problem Areas

Time and attendance for staff and students during 'stampede' (morning drop off, evening departure) for payment, insurance and knowledge purposes.

Verifying new teaching staff/support staff/security staff as trustworthy individuals.

Non recognition of new teachers/new students. Non- recognition of parents and others associated with school leading to reduced throughput rates/unacceptable access. Communication dependant on physical proximity to phones etc means time lag. Ensuring right people have access to canteen/library facilities.

2.2 Student Perspective

Problem Areas (regarding identification needs)

Students were concerned with a secure place (cannot be targeted successfully by bullies or malice) to store documents and corrections as well as messages from teachers/support staff and other students.

It was also felt that preventing identification of those who do not have resources (or have resources) to pay independently would decrease incidence of bullying.

Throughput was considered a problem in Library's/canteens because of identification needs at counters. Students were aware of inability to use tokens/passwords/PINs by those with disabilities and loss/theft (target for mugging) was also considered problematic.

Notice board facility was not thought to be privacy enhancing (lowering self esteem, target for bullying).Restricted access to facilities as a result of being 'tarred with same brush' was not seen as a solution. Non recognition of new teachers/students diluted a sense of community in the school. Non continuity of work between changing teachers was problematic especially for final year students. Advantages of elearning are not possible when supervision during access is dependant on experienced staff.

2.3 Teacher's Perspective

Problem Areas (regarding identification needs)

Verifying student identity in corridors/classrooms and for the submission of work done on computers (preventing plagiarism between students) was particularly important for teachers. Verifying adult/teacher identity was also difficult in the face of a high turnover of staff. Easy continuation from previous teachers work with students required 'identification' of work done. Easy secure access to employment/pension/personal details on a secure storage resource is highly desirable. Access to canteen/library/other facilities is dependent on tokens/personal knowledge and continuity of knowledge among support and security staff was also considered problematic. Inability to make use of e-learning environment when plagiarism or use of false identity cannot be confidently eradicated.

2.4 Parents Perspective

Problems areas (regarding identification needs)

Parents felt concern regarding recruitment system for staff in school. Low confidence was also expressed over access rights to information about students.

Another area of concern is alert and response if a stranger is on the property, property is stolen/destroyed or if a student is mistreated. Recognition of teachers is also felt to be difficult.

Current System response

The current system (focusing on identification) includes swipe cards and passwords. Traditional phone systems and email are available (where available). Restricted access rules (physically locking areas/utilities) are implemented.

There is a strong dependency on personal Knowledge of staff which in turn is dependent on continuity of staff experience. Cooperation of students and availability of staff is critical. Education and training needs to be reiterated for new staff and students. There is a time lapse before familiarity of staff was effective. Trust is felt to play a significant role in exchange of information. Waiting for replacement tokens and use of alternative systems tends to mean relying on peers and staff. Alternative arrangements made some students feel isolated.

3. Motivation for focus on identification needs in a Secondary School

Central to management of user group needs in an education environment is management of identification needs. These needs have escalated over the last five years particularly from the following pressures:

- Low confidence in recruitment process, special consideration for prevention of unacceptable access to a school environment by individuals who present a danger to vulnerable people.
- Increase in numbers of students (higher throughput requirement) with changing needs (varied curriculum's and activities) attending schools but retained dependence on traditional methods of communication within the school (personal knowledge, telephone, sometimes email). This means lower communication opportunities in the face of greater demands.
- High attrition rates for teachers and administration staff especially in underprivileged schools means continuity of knowledge is lost. Management of 'legacy' requires a core identification system be in place.
- Broader education opportunities (elearning initiatives) depend on correct identification.

4. Solutions Selected and Reasoning

The following solutions were recommended. Vendors have been selected and work is ongoing for system integration and implementation. Solutions focused on practical needs taking into consideration each user group perspective. Policies governing the use of selected technology were also developed in accordance with the data protection act as well as best practice principles.

4.1 Radio Frequency Identification - RFID (proposed for portal entrances to school)

This technology is focused on the use of smartcards containing a computer chip which is activated using an electromagnetic field using a strong radio frequency from a RFID reader. The chip will not contain any identifying information regarding the holder. A dispensing machine will be located in a supervised area.

Application – RFID cards and mobile RFID reader unit

RFID cards are considered to be the only solution applicable to the problem of 'Stampede' times for students and staff. RFID cards are expected to enable identification of those who are on school property. At these times, it is possible that the entire school population may pass through the school portals within 10 minutes. This is very important not only for time/attendance records but also in circumstances such as fire drills. To preserve resources and increase throughput, implementation includes a 'time lag' scenario whereby, RFID holders submit to one of few iris system modules before using RFID card to access one of many available PCs (identification first, followed by authentication).

Faster access for students and staff to canteen, library when used with facial bank technology (flashing card in front of RFID reader, allows system to connect to facial databank and brings up facial photograph allowing for staff to check and authenticate individual for service). Staff carrying the RFID reader unit can check and register immediately who is in corridor.

Identification Concerns and Benefits

Low security unless part of combination system because smartcards can be lost/forgotten/stolen and swapped. This means they do not help prevent intruder access, but when combined with a counter mechanism (a light ray mechanism which counts number of people passing into school at portal), can help alert staff. RFID cards can work to deliver high security after crossing school perimeter when used in combination with an iris recognition system (for access to communication network/facilities within the school) and facial databanks i.e. for roll call at beginning of classes. Student and staff access to notice board/timetable/message service can be enhanced by using a combination of authentication (token – RFID card) and identification (submission to iris recognition system). Mobile identity checks combined with facial databanks reduce potential for confrontation or incorrect identification. Throughput for library, canteen services can significantly improve with less dependence on personal knowledge of staff member. The technology is convenient in that it incorporates customary use of photos – meaning training requirements are kept minimal.

4.2 Iris Recognition Systems (fixed and mobile) located strategically around school

A biometric sample is a unique and linguistically neutral value representing a biometric characteristic of an enrolee as captured by a biometric system. Biometrics such as fingerprints or irises cannot be easily lost or stolen. Iris recognition systems use the human iris to capture a biometric sample for processing into a format that can be used for identification or authentication. Iris recognition systems have been proven to have the greatest reliability in comparison to other biometric systems.

Application

Students and staff submit to an iris recognition system unit which uses the data result to check against a central database for a match. When a match occurs, access to required facility is allowed. Iris scans are planned for access to sensitive information (as agreed by students and staff) and incorporated into logging mechanisms for enabling use of technical devices. Mobile iris recognition devices can be used for immediate enrolment/verification of an individual who may not be required to enrol on school database.

Identification Concerns and Benefits

Iris recognition units are expensive and require 1 – 2 minutes supervised enrolment (longer for younger individuals). Enrolling however incorporates learning for future eye scans that take 2 – 3 seconds. Strong safeguards must be in place to prevent searches not initiated by school. Participants must be cooperative and the system is not suitable for high throughput requirements at 'stampede' times. Suitable for time/attendance for staff at different locations in school.

Can enhance sense of privacy regarding access to portfolios of work and sensitive information. Easier management of staff is possible (through centralised access policies). Message system can be monitored for problems with fewer resources (when logging system is adequate). A unit can be made available as an alternative device in canteen/library if RFID option fails. The iris recognition system can prevent unauthorised RFID card distribution as a log can be kept. Regarding, mobile iris recognition units – these can deliver the same functionality as fixed devices but access needs to be secure (submit iris code). The device can be prevented from working if not located within or close to the school parameter but wireless technology presents other security considerations. Those coming to school for short periods (to work as casual labour etc) can be enrolled on an ad hoc basis.

4.3 Facial Data Bank (Portal and Mobile)

Photographs of students and staff are stored on a centralised database.

Application

The photographs of students/staff are taken and made available to RFID mechanism.

Identification Concerns and Benefits

The system is still dependent on judgement of staff when photos are being viewed (for verification) and students will need to enrol perhaps once per year to allow for changes in appearance. The facility is also capable of being used as an alternative if RFID or the iris recognition system fails in the case of roll call or in canteen/library environments. Little or no training is required to use the system (intuitive) and enrolment photos are always acquired.

4.4 School Management System

A database system that stores and locates data for users, allows messaging and provides management tools. A school management system for user groups was selected based on the easy integration and implementation of chosen identification systems.

Application

The school management system focuses on time/attendance of students and staff, personal portfolios for individuals with secure access, notice board capability – students need only

'flash' RFID cards in front of a networked PC to let them know their current timetable and if they have mail (which they can then access further using iris scan) and a messaging system (which potentially can be linked to mobile phones for parents letting parents know of arrival of students onto school grounds).

Identification Concerns and Benefits

Security risks are posed by internal resources and most likely related to lack of training or skills. When biometrically enabled together with agreed management policy, the system becomes very secure and privacy enhancing for each user group.
Time is required for adaptation, installation and testing.

The system has been designed for intuitive use and tested in Spain, Italy and Finland - training is minimum (if user is already familiar with using internet browsers).

5. Impact on typical day scenarios for user groups

5.1 Principle Administration

Make required changes to timetables and send messages.
Statistics are checked for time and attendance (designed for ease of use but only available to those with appropriate access). The results of the system (including discrepancies with roll calls) can be checked before parents are informed through mobile phones etc. Senior Administrators enrol new staff or students (checking staff against external database for trustworthiness of individual and receives confirmation of acceptability). Training for use of system as part of school orientation efforts is provided.Data affecting Insurance/safety can be quickly viewed for management/audit purposes.

5.2 Administration (non principal staff)

Staff enter School through RFID enabled doorway with card immediately registering time of arrival. Use iris system for time/attendance purposes and access to work.
Recognise and greet new staff member or teacher/student (email with photo ID attached). New staff member submits code for time & attendance. A student has lost/forgotten RFID card and requests to use iris system for print out of new card.
Staff can check with facial databank once iris has been submitted and accepted for new card replacement. To prevent damage and ensure correct usage of iris recognition system, staff observe use.

5.3 Student

The student enters School through RFID enabled doorway with card immediately registering time of arrival. Checks messages/timetable quickly (flash RFID card in front of monitor for instant access to timetable view and sees simultaneously or not any messages need to be collected). Observes new teacher (facial photo and name) will be taking next class and that a new student has joined the class. Greets new student. Student finishes class and submits homework for teacher after using iris recognition system and then RFID card. Students uses RFID card to purchase meal and take out books from library. Canteen/library staff can see photo of student using RFID and facial databank. Alternative system of iris code in place if necessary.

Student takes eLearning class and test by using RFID for enrolment to eLearning class and iris system for enrolment to test. Student exits school environment RFID card is recorded as having exited school.

5.4 Teacher

The teacher enters School through RFID enabled doorway with card immediately registering time of arrival. The teacher then uses iris recognition system for official time/attendance. Check messages/timetable quickly through RFID card. Access using iris recognition system to messages and sees new teacher (facial photo and name). New student has also joined a class.

Teacher goes into class and recognises new student. Welcomes student to class. Calls roll and can see if RFID data matches up with those present in class. Teacher finishes class and wants to change class requirements/ homework details for students. This is done by using iris recognition system for access to portfolio and messaging system. Teacher greets new teacher on corridor. They see two students running, late for their next class. The teacher approaches using a mobile device that registers RFID cards and can call up a facial databank with names. The students are stopped using their names and the incident is recorded instantly.

The new teacher supervises an eLearning environment and without knowing any of the students can check their ID. In a test environment, access is through iris recognition system. Students cannot change seats during test – iris verification is possible during test by teacher using mobile device to check individual sitting at PC and RFID card they are carrying. Teacher has access immediately to results of tests and having drawn up statistics can release the results for collection

5.5 Parents

Parents can potentially be assured that student has arrived safely to school by mobile device and also be informed when student has left. Parents can feel more confident about recruitment policy. The need for the student to carry cash is reduced. Potentially can ensure only authorised person collects student from school.

6. Usability for user groups – Concerns for proposed system

Priority concerns for each user group were focused on several questions. The answers to these questions formulated management policies. These questions include – How technically secure is the system?,Who has access to what information? How will biometric data be used?, What policies are in place to enhance privacy/legal obligations (including misuse, correction of data, length of time held?

All concerns for user groups are rooted in privacy fears. The system is non-mandatory so these concerns form essential design parameters for the system. In considering appropriate policy, current regulations within the UK and EU were taken into account. Policies were also influenced by examples from around the world – such as Children's Online Privacy Protection Act (COPPA) in the USA (COPPA, 2000). These policies are open to adjustment and expansion based on how each user group experiences the system. Basic policies for all user groups abide by the Data Protection Act (DPA) which governs the use of personal data in the UK (Data Protection Act, 1998).

6.1 Effect of Data Protection Act (DPA) on user groups

All collection of data (that can lead to identification of individual) must have the consent of the individual before processing. This is no different from present requirements by law for the school however as the system includes the use of biometrics, the school must consider itself dealing with 'sensitive data' which extends these requirements. Explicit consent of data subject or if under age, guardian's consent, is required for enrolment of biometric and processing of biometric data. In the case of staff, collection and processing can be included as

part of employment contract. As enrolment is voluntarily, however the same explicit and verifiable consent is required. Even information the school has traditionally been entitled to collect can cause objection. These pressures require that Privacy Policies within the school be carefully considered.

Purposes of collection must be specified to data subject and/or Information Commissioner (appointed by the crown) and adhered to (fairly processed according to the DPA and according to common law rules of confidentiality). A clear and easily available privacy policy is essential for each user group. A particular concern for biometrics is that as a unique identifier, it can be used to link across disparate databases. If the system is 'two way' (i.e. searches can be carried out by agencies other than the school, there is the increased likelihood of 'dragnet searches' not triggered by evidence of wrong doing. There is a continuous burden of proof placed on staff (contrary to a legal system which supports innocent until proven guilty). Due process of law and right to contest results may be affected. Results also rely on correct maintenance of data and can be prone to omission, preventing the 'full picture' coming to light. Staff can request the data controller not to process personal data unless it is included in a contract. If quality of data is unreliable, there is the risk of a match. The individual is at risk of being denied 'due process of law' (notice of situation and the right to contest results).

The organisation collecting/processing data must also take 'reasonable' measures (security) to prevent loss, unlawful processing, theft, damage or destruction of data. The security of biometric data is particularly critical as once it is lost, it cannot be replaced without complete re-enrolment (assuming images are not being used).
Portfolios (which would contain information normally collected within schools) may become more vulnerable to security breaches when databases are networked and located centrally. New management skills will be required.

7. Privacy Policies Recommended for User Groups (in addition to DPA compliance)

7.1 Parents (regarding data subjects under age of 18)

- Expect requirement for prior, verifiable consent for the collection, use and or disclosure of personal information from those under 18
- Offer objective training or access to training for privacy rights and new technology as impacts data subjects
- Upon request, provide a parent with the ability to review the personal information collected from an under 18 person
- Provide parent with the opportunity to prevent further use of personal information that has been collected already or future collections
- Be specific about 'processing'
- Explain clearly any 'conditional participation' (whereby those under 18 can participate in an activity only if they provide more personal information)
- Establish reasonable procedures for concerned parents

7.2 Students (in addition to normal compliance with DPA)

- Provide objective training in privacy and the use of new technology that impacts the student.
- Provide clear information on what information stored in personal student portfolios is open to parental access (some students fear excessive access by parents which could reduce creativity and productivity in subject areas such as Art, English, and Religious Studies).

7.3 Teachers and Administrators as 'data subjects' (in addition to compliance with DPA)

- Define what it is that needs protecting for Teachers and Administrators and make sure system can not be used for 'two way' purposes. Ensure a match result is immediately communicated to the staff member concerned.
- Require clear information on what happens to biometric data if it is used in conjunction with an external database including result and procedure if a 'match' happens. There is concern that a 'chill effect' on creativity and productivity will happen if staff feel they are being monitored.
- Require objective training in privacy and the use of new technology that impacts staff. This encourages a positive approach to systems that would make work lives easier.
- Elect a representative who can check for data trails and uphold the interests of teachers.
- Check contract for conditions of employment regarding expectation to privacy.

7.4 Administration acting a 'data controllers' (in addition to normal compliance to DPA)

- Ensure sufficient and secure logging resources using iris recognition where appropriate. Combine this with security policies including fine-graining user access and locking user rights and access rights together.
- Require definition of role and purpose of staff looking after data warehouse and software. Check that conditions are observed as part of contract agreement.
- The school must at all times be able to prove it took reasonable steps to prevent unauthorised activity by employees using the school management system. The school can be held vicariously liable. Employee contracts must specify what is acceptable and unacceptable and the right of the organisation to monitor activities where its assets are used. What exactly results in disciplinary procedures and summary dismissal should also be specified in the contract and an obligatory separate form should be signed accepting these policies.
- Prevent use of system for data mining purposes.
- Administration must incorporate vendor vigilance so that DPA principles are observed but also understand the effects of remuneration from outside vendors and have a policy regarding how to deal with such communications. Incorporate contractual obligations that protect school data even when sale or merger of vendor takes place. Ensure that data is protected even when bankruptcy of vendor occurs (which can encourage the sale of data to marketing organisations).
- Ensure access by police or state to data held by vendors is not useful.
- Be aware that increased sense of control can create a 'chill effect' that reduces motivation and productivity.
- Create individual responsibility (and the ability to be responsible) for keeping personal information up-to-date.

7.5 Vendor Organisation (in addition to normal compliance to DPA)

- Be aware (anticipate where possible) of growing legal obligations particularly regarding sensitive data such as ethnicity. All data that can be linked to the age of an individual that is under 18 should be treated as sensitive data.
- Do not take actions that could infer inconsistency with legal or contractual obligations especially with regard to transfer of data.
- Be specific about what will happen to sensitive data (which can be viewed as an asset) during sale, merger or bankruptcy proceedings.
- Provide extensive privacy policy details (that identifies vendor by name and provides contact details) easily accessible through user interface or available as hardcopy.
- Policies that condition participation must have the agreement of the school.

7.6 Technical policies supporting privacy enhancement

The following is representative of basic technical security parameters built into system parameters.

- Prevent transfer/comparison with external database unless initiated by school.
- Ensure no access to database following installation without submission of recognised/accepted iris.
- Require iris submission for all access/changes to system portfolios.
- Ensure access and user rights are fine grained according to iris codes
- Ensure all those designing/administering to database are registered on database and exposed to same checking procedures as school teachers and staff.
- Prevent student database from mixing with staff/teacher database.
- Combine RFID with iris recognition for identification and authentication where content is considered private.
- Ensure submission of iris before new RFID card is printed (prevent multiple cards per individual)
- Do not store identifying data on card.
- Do not allow access to individual information/services based on only card possession (combine with facial databank and/or iris system)
- Ensure RFID card dispenser is in full view of staff at all times.

References

Childrens Online Privacy Protection Act, 2000 USA.

Data Protection Act, 1998 UK.