

Contents

1	Introduction	2
2	Evaluation of the current system	3
2.1	The current system	3
2.2	Evaluation	4
3	Biometrics systems	6
3.1	Efficiency of biometrics	6
3.2	Voice Recognition System	7
4	Implementation of the new system	9
4.1	Implementation with Voice Recognition System (VRS)	9
4.2	The privacy issue	10
4.3	Critics and improvements	10
5	Conclusion	12

Chapter 1

Introduction

Traditional approaches to secure access are based on “what you have” (tokens), “what you know” (PINs) or both. These methods bring with them their collection of issues. Tokens can be lost or stolen while passwords may be forgotten by users, reused for different applications or even written down.

Biometric technologies tend to address the problems of the traditional approaches by using biological traits or behavioural characteristics to identify an individual.

As for validating an individual’s identity, there is a distinction between *verification* and *identification*. *Verification*, resolves the question “Am I who I claim to be ?” by denying or confirming the claimed identity. *Identification* involves establishing an individual’s identity, therefore answering to the question “Who am I ?”.

Among the features used to achieve *identification* and *verification* are fingerprints, hand geometry, iris, face or voice recognition. No two individuals are alike. Therefore, by being irrevocably tied to the individual, biometrics seems to effectively address current problems and to also bring many advantages. However, emerging technologies often promise more than they can deliver. This is why a very critical approach will be carried out to evaluate the suitability of biometrics with Cedars Upper School’s needs, in terms of security and usability.

Furthermore, as biometrics is a technology that deeply deals with people’s identity, the often neglected issue of privacy will be considered carefully in order to avoid any collected data to be misused.

Chapter 2

Evaluation of the current system

Currently, Cedars Upper School allows free access to most areas of the school. Where access restrictions is required, it relies on manual keys held by relevant staff.

2.1 The current system

Cedars Upper School hires a security officer. There is currently no CCTV deployed on the school area.

The first perimeter is defined by the entire school. It is only open to the public during hours of operations (9am to 5pm, Monday to Friday). The school is otherwise closed. The main gate, which is the only point of access to the school, is otherwise locked by a manual key. Each member of the staff is given a key to access the school out of the class time.

The main building defines the second perimeter and contains both the classrooms and the staff offices. However the security officer is present at the entrance of the building to avoid unauthorized individuals to penetrate this restricted area. The identity of the students is in fact never checked. During the lunch break (1pm to 2pm) the building is locked and students are asked to leave. Members of the staff are given a key to still be able to access their offices.

Classrooms are locked when not in use. They all have the same lock that members of the staff do not need to carry a different key for each classrooms.

Offices are only accessible by the teachers they are used by.

The library, which is located next to the main building, can be accessed at any time during hours of operations. Otherwise, it is locked by a key which is only given to the library's staff. Prior to make a reservation, teachers can still be granted a key, for a given period of time, to get access into the library out of the opening hours.

This access control system has been set up when the Cedars Upper School was build. However, the restrictions of access, based on time slots, have been defined more recently, after degradations of classrooms and walls of the main building occurred.

2.2 Evaluation

Even if the current system tends to be strong, it suffers from the following issues:

- Teachers often forget to close classrooms or to take their keys before going to the school
- There is no knowledge of who accessed the different areas. The reservation system to obtain a key for accessing the library during the week end is heavy to manage and does not satisfy the staff members. The fact that these borrowed keys can be copied shows that the system is not effective.
- The security guard makes use of a set of master keys to allow him full access more easily. If lost or compromised, this requires the change of all locks, which would be very expensive.
- The fact that the locks used for the classrooms are all the same (to allow a unique key to open any of them) has the same issue than the use of a master key.
- The access system too much relies on the unique security officer (opening and locking the doors at the given time slots, assisting staff members who forgot to take their keys, etc). If he is absent, numerous issues such as delays are likely to occur.

- Attendance checking is not carried out, thus allowing students to miss class without the staff to be notified. students may still stay in the building no control of

Chapter 3

Biometrics systems

3.1 Efficiency of biometrics

Most of the studies on biometrics are evaluating the efficiency of different systems with regards to their False Rejection Rate (FRR) and False Acceptation Rate (FAR). A False Rejection happens when an enrolled user is not recognized by the system and is therefore not granted access. On the other hand, a False Acceptation is the event of a user whose biometric features are not registered in the system to be granted access.

The FAR and FRR of products, because they are usually published by the vendor themselves, are likely to not be utmost critical. The Darmstaedter Fraunhofer-Institut, in collaboration with the BSI (German Federal Institute for IT Security), have run series of tests on different biometrics systems that were given by vendors in 2001. Obviously because of pressure from the same vendors, the results of this independent test were never published.

During the past years, many [CT,2002] [IBG, 2003] [Putte,2004] [Schneier, 2005] [SF, 2003] tests have been conducted to break into biometric systems by creating fakes fingers, faces, voices or iris. With more or less efforts, almost all systems that went through the tests have been defeated. Technologies to detect the liveness of the presented features are being developed and implemented into the different readers to avoid such deceptions.

This all means that biometric systems are far from being as secure as they are claimed to be. If the security is the first issue concerned by the use of such systems, a not less important issue remains: the usability. This is why, by focusing on voice recognition, the next section will explain more about it.

3.2 Voice Recognition System

To avoid any confusions, it is important to understand that speech recognition is concerned by “what is being said” while voice recognition or speaker recognition aims at finding “who is speaking”.

As far as voice recognition is concerned, two different categories [Bergdata] [Triradius, 2002] are to be defined: *text-dependant* and *text-independant* voice recognition.

- **Text-dependant:** a specific phrase is used by all speakers, and the system is trained on that basis.
- **Text-independant:** the system is trained to recognize the speaker independant of what phrase they utter.

The need of carrying a token or knowing an identifier with *verification* systems brings an additional security because the token itself is not enough to get access as well as faking the feature is useless without having the token. *Identification* is much more convenient because there is not token that might be lost or forgotten. However *identification* systems are slower on large scale deployment, it would not make any difference for a small environment such as Cedars Upper School.

Text-dependant is the easiest type to implement because users enrollment takes only few minutes and users always say the same speech. However, this is also the much easiest one to defeat with advanced sound recorders. On the other side *text-independant* brings more security because a deception with a sound recorder is practically not achievable. The main problem is the enrollment for *text-independant* takes on average two to three hours per users. Also, if the use has to read what text has to be said, an additional amount of time is required for each authentication.

On top of having to choose between *verification* and *identification* as well as between *text-dependant* and *text-independant* the following list of issues [EEE, 2002] have to be taken in consideration:

- Microphone position: not everyone has the same height and this has some consequences in the voice if the users for example have to bent.
- Accoustic environment: the echo in a hallway or any other noises that can be generated by the environment (other students speaking, weather conditions, etc) are particulary disturbing the recognition of the voice.

- Emotional state of the speakers: for many different reasons such as a stress before an exam, the voice can be distorted and therefore not recognized.
- Voice aging: teenagers voice is likely to change substantially during a school year. This issue might involve a re-enrollement to be required over time.
- Non-acquirable feature: some students might be mute or even simpler have their voice “broken” due to illness

Since the aim of the upgrade of you system is to increase security and monitor student attendance, voice recognition is obviously not the biometric that we would recommend to Cedars Upper School. The security requirements would involve the choice of a *verification* system with *text-independant* voice recognition which both bring their collection of drawbacks. The time required for the enrollemnt, added to the time wasted for attendance checking before each class would bring far more troubles than advantages and it can almost be predicted that the system would be given up short after its installation.

Chapter 4

Implementation of the new system

4.1 Implementation with Voice Recognition System (VRS)

Using voice recognition, we would recommend the following implementation:

The VRS does *identification* and is *text-independent*. Before switching to the VRS, students will enroll to train the system to their voice for three hours.

- Access to the school through the main gate remains without access control
- For both students and staff members, entering and leaving the main building, its classrooms or the library requires to go through the VRS.
- For offices, the VRS allows teachers to only access the office they work in.

Besides classtime, the VRS will only allow the staff and will reject any student attempt to access any building. This means that, at any time, any member of the staff can access the classrooms or his office. Instead of a key reservation system to know who accessed the library during the week end, the access logs of the VRS can be checked in case of an incident to happen. The students will only be allowed access to classrooms according to their schedule. Before each class, they have to go through the VRS as proof of attendance. A monitoring tool allows the administration to watch a real-time

attendance report.

Furthermore, the whole system (devices, doors locks and servers) alimentation is provided by a UPS to keep it up and running in case of power outage. In case of a fire alarm, all doors will automatically get unlocked to allow a quick evacuation.

4.2 The privacy issue

Privacy has always been an issue when personal data are being collected. The key to cope with that issue is to make the users aware of what data will be collected, what they are going to be used for, how they will be stored and for how long.

Regarding the purpose of the system (security and attendance monitoring) the data to be collected shall be the following:

- The pattern of the users voice
- The attendance of the students for each class
- For each user, when they went through each access control

Making sure that machine collecting all the data remains secure is the first key to privacy practice. The patterns storage can not be avoided. The attendance could possibly be deleted after a given period of time but since they are also likely to be recorded into administration registry, there is no real point to do so.

Recording people's incoming and outgoing at the different access control points is what may indeed concern them the most, with regards to their privacy. The problem is that these data are collected because they would be very useful to get clues after an incident happens at a given area and period of time by determining who was then present. But since incidents are usually detected quickly and the data therefore checked shortly afterwards, there is certainly no real point to keep them longer than two weeks.

4.3 Critics and improvements

In theory, the VRS implementation shall fulfill both the security and the attendance monitoring requirements of Cedars Upper School. However, such an implementation is practically very likely to fail because of the problems of usability (microphone position, acoustic environment, emotional state,

voice aging, etc) that voice recognition systems suffer of [EEE, 2002]. The amount of time wasted due to false rejections before and after each class would very quickly annoy both the staff and the students. Users do not like changes and are only likely to accept them if they bring benefits rather than frustration.

An improvement would be to replace the VRS by either a fingerprint or a hand geometry system because their false rejection rates are much lower [Secugen, 2003] and the enrollment far quicker. Furthermore, by increasing the number of readers and therefore allowing concurrent controls to happen, the amount of time spent for each control would significantly reduced.

Chapter 5

Conclusion

It has been clearly shown that voice recognition is not the technology to go with, for Cedars Upper School. Using other biometric systems would bring some improvements in terms of usability and efficiency.

We would recommend to opt for the accuracy and low FRR of either fingerprint or hand geometry recognition [FCW, 2000]. However, we do advise to not switch the whole access control infrastructure to a biometric system as unexpected problems may still happen. We also strongly recommend to opt for a solution that the entire population may use by providing an alternative solution for disabled persons (handless, mute, etc) or exceptional events (injured fingers, etc). The solution to this might be multi-modal biometric system where users are for example offered to be checked either against their iris or their fingerprint.

Bibliography

- [CT,2002] Thalheim Lisa, Krissler Jan, Ziegler Peter-Michael, c't Magazine, November, 2002, August 21, Koerperkontrolle, Biometrische Zugangssicherungen auf die Probe gestellt, p. 114. Retrieved November 9, 2003, from <http://www.heise.de/ct/02/11/114/>
- [IBG, 2003] Tsutomu Matsumoto, 2002, October, Importance of Open Discussion on Adversial Analyses for Mobile Security Technologies, A Case Study for Identification, International Biometrics Group. Retrieved November 9, 2003, from <http://www.itu.int/itudoc/itu-t/workshop/security/present/s5p4.pdf>
- [Putte,2004] Ton van der Putte, 2000, September 21, Biometrical Fingerprint Recognition: Don't Get Your Fingers Burned, Esire, an Origin Extended Enterprise. Retrieved November 14, 2003, from <http://cryptome.org/fake-prints.htm>
- [Schneier, 2005] Ton van der Putte, 2003, November 15, Hacking Fingerprint Readers, Crypto-Grams. Retrieved November 16, 2003, from <http://www.schneier.com/crypto-gram-0311.html#9>
- [SF, 2003] Harrison Ann, 2003, August 13, Hackers Claim New Fingerprint Biometric Attack, Security Focus. Retrieved August 14, 2003, from <http://www.securityfocus.com/news/6717>
- [Bergdata] Gerek Alexander von Graevenitz, About Speaker Recognition Technology. Retrieved January 24, 2004, from <http://www.bergdata.com/downloads/Introduction%20to%20Speaker%20Recognition%20Technology.pdf>
- [Triradius, 2002] Triradius, May, 2002, A Speaker Verification System. Retrieved January 28, 2004, from <http://www.ece.uvic.ca/499/2002a/group05/development/progress1.pdf>

- [EEE, 2002] School of Electronic & Electrical Engineering, University of Birmingham, 2002. Retrieved January 28, 2004, from [Speakerhttp://Recognitionwww.eee.bham.ac.uk/russellm/OHP14_Speaker_Recog_2002.pdf](http://Recognitionwww.eee.bham.ac.uk/russellm/OHP14_Speaker_Recog_2002.pdf)
- [Secugen, 2003] Secugen, Biometrics Overview, 2003. Retrieved January 24, 2004, from http://www.secugen.com/support/tech_bio.htm
- [FCW, 2000] Michelle Speir, June, 2000, Biometrics: More than a helping hand. Retrieved January 29, 2004, from <http://www.fcw.com/fcw/articles/2000/0605/tec-bio-06-05-00.asp>