

Do Biometrics have a role for school registration?

Abstract

Biometrics is very much still in its infancy, still not a publicly accepted technology. The country as a whole is divided on its use with particular reference to their role with national identity cards.

This paper outlines my key objections for the use of this technology for the purposes of school registration. Which are:-

- *Children from a young age see giving up their finger print as a natural day to day occurrence without understanding the potential consequences.*
- *I would query the effectiveness of this new system, on accuracy and timely delivery of attendance records in the event of a school emergency evacuation*
- *No system can guaranteed the security of information against future technology. Attempting to protect life time relevant information is extremely tricky and potentially costly.*

There is a great possibility that within ten years time the present Chip and Pin will be replaced by perhaps Chip and Print. Our thumbprint becomes the pin, but unlike the pin it can't be changed it's with you for life.

My Credentials

I've worked in the computing security field for the last eight years, working for the likes of Cisco Systems as a Lead Architect for their network access control solution, protecting 99% of the fortune one hundred companies from network attack. This has given me the opportunity to work with the likes of Visa, Fidelity, and Meryl-lynch to implement security systems that are both secure and workable.

The Case

One of the key benefits I get by sending my children to school, is they learn social interaction and key life skills such as discipline and responsibility. Everyday they take responsibility of their snack money, remembering their PE kits, home work etc such learning is key to later life. The patterns of activity we develop during your early years clearly set the tone for how we evolve and behave in later life. By encouraging our children on a daily basis to give out their thumbprints leads them to think this is a natural activity. Who else will they give their biometrics too, without consulting their parents and asking questions like why, and what will it be used for?

As a parent I make decisions for my child on a daily basis some will affect their lives for the next few minutes others will potentially affect the rest of their lives. A decision to allow my child's biometric information to be taken is a life long decision; they after all can't change it. Technology advances in leaps and bounds it is impossible to imagine all future possibilities and thus when making a decision that has implications far into the future you can't make them based on what can be achieved with today's technology. For me it comes down to the whether the benefit outweighs the implications.

When replacing any existing system it is often easier to see how a new system fixes the short comings in the existing system, but often its the case that any new system also comes with its own set of weaknesses some of which were not immediately evident.

For instance with proposed system, each child is expected to place their thumbprint on the machine daily. There is no carrot to make them do this, and equally there is no guarantee that the scanner will

read the print. Scanners fail to read prints when they are dirty or that the child themselves has perhaps damaged their thumb print via a scratch or other abrasion. So such a system needs a backup strategy, the one currently being proposed is that the Admin staff at some point will print the role call and then confirm by visiting each non fully attended class room that the print out is in fact an accurate record. What's interesting here is when is registration deemed over ?

This then leads to the question how long will the overall registration process will now take...Currently each teacher takes his/her own register, this is happening in parallel. The proposed backstop is a largely a sequential process. This obviously means it will take longer to provide full clarity of who is present in school. Not a problem for issuing attendance certificates at the end of term, but perhaps a big deal for emergency evacuation.

Issues that will effect this time are

- Admin staff busy dealing with another task
- Printer jams, or out of toner/paper
- Computer crashes
- Power loss in the building
- Network failure
- Scanner fails in classroom

These risks are in stark contrast to the traditional method, where the risk is limited to a pen not working...

So an evacuation at the start of the day might not provide clarity of who is in the building. Whilst in the existing system it may be possible for one teacher not to provide clarity it is hard to see a scenario where all teachers do not have complete clarity. This is the key facet behind the success of any fault tolerant solution, distribution. The system being proposed is heavily centralisation and thus opens the possibility for single point of failure, something that is avoided in all critical systems.

The school has a legal obligation for duty of care; it therefore seems right that any new system is as robust as any previous systems.

It is highly possible that in less than ten years time Chip and Pin will be replaced by perhaps Chip and thumbprint. We will see the use biometrics to protect the things we most need to protect. Like all forms of password protection we are encouraged to keep this information private, in fact we are told to destroy any paper copies. Obviously banks keep this information in some form in order to validate our identity at the point of transaction, this information as you can imagine needs to be kept extremely securely. However we all know that what ever measures are taken this information can still be potentially hacked or stolen, a banks database is too much of a temptation to a would be hacker. In the case of a compromise in security the bank has to spend a lot of money issuing new cards and pins, but the problem can be fixed. Now imagine the case where the burden of proof is your thumb print, hmmm not an easy thing to change.....

Now imagine that hackers did not have to crack a banks computer they could hack small businesses, local library or even a schools computer and obtain information such as

“Name” , “DOB” , “Thumb print” , Parents names , perhaps in some cases even Mothers maiden name....

Whilst some of this information is already stored on a schools computer, there is some valid justification to why it is kept. In fact the Data protection act requires organizations to only keep information that is deemed necessary, other information can be removed on the request of the individual or guardian in question.

Currently there is little to no reason to hack a schools computer, but in the future the trade of biometric information may be as common as spam or mailing lists today.

Identity theft is on the increase only recently credit reference agencies are selling services to inform you when a credit check is made against you, thus alerting you to the possibility that perhaps it is being made not from you but by a person impersonating your identity. Information about a person's identity is seen to be highly valuable, especially in the wrong hands.

Now bio companies will tell you that the print is not stored as an image, and that's true. However the data that is stored is sufficient to compare it against a print received when the child registers every morning. The information is therefore sufficient to determine what the print looks like, and thus is not beyond the bounds of possibility for some one to extract the key factors used to identify the print. From this information it is possible to produce a gelatin based print to lay over a persons existing print. Hackers have already demonstrated they can make a home made print, using basic household technology, (not so Mission Impossible...)

They will then tell you that it's still ok because it's encrypted with a 128bit key, and that will take millions of years to crack. Again to some degree this is true, but all it really means is that if you were to try every key combination it would take that long. Hackers don't approach the problem in this way, for example the German Enigma machine used in World War II boasted similar levels of security but what they failed to consider was the fact that the number of keys to try could be greatly reduced once you have some understanding of what is being encrypted and how it is being used, this then provides a means to greatly reduce the number of keys to try. Another way in is the fact at some point in time the information that is encrypted becomes unencrypted in order to perform the finger print match, it is therefore possible to extract the data at that point.

IBM is currently investing heavily in trying to secure biometric information for this very reason; they know it is just a matter of time before it is broken. The term "matter of time" is important, as sometimes is the case by the time the information has been hacked it is possibly redundant or easily made redundant by changing E.g. a PIN, but in the case of biometrics they are with you for life.

I therefore feel that there is an element of risk storing thumbprints on a school computer. Again consider the risk/benefit, from a parent perspective I see no benefit. My child is registered in school, he and she has been registered in school for the last 2-4 years perfectly satisfactory so Im not getting anything extra, for exposing my child's identity to some level of risk

Whilst this paper only scratches the surface of the issues behind biometrics in schools for registration, I hope it raises enough concerns to come to the conclusion that their role should be rejected, since they create a whole host of new risks and problems with no obvious parental gain. In fact when considering how much it would cost to build a fully fault tolerant solution it may cost the school a substantial amount of capital investment.

For me the take away thought has to be does the benefit justify the risk, to date I have not seen any substantial evidence to suggest that to be true. I would also think it would be reasonable to know that other solutions have been explored.

Andrew Clymer
Tel. 01249 655859
(andy@beaconsoft.co.uk)

References

Security Issues

IBM's quest for greater biometric security, "Its just a matter of time for it to be hacked"
<http://www.techworld.com/security/news/index.cfm?NewsID=4238>

How to crack biometric encryption
<http://www.site.uottawa.ca/~adler/publications/2005/adler-2005-AVBPA-biometric-encryption.pdf>

DIY Thumb prints
http://www.ccc.de/biometrie/fingerabdruck_kopieren.xml?language=en

Old PC's a goldmine of information
http://www.theregister.co.uk/2004/09/03/old_pcs_not_wiped/

Credit Card Companies keep ID theft secret
http://www.theregister.co.uk/2005/09/24/data_id_theft_secret/

Biometrics fail to secure prisons
<http://www.schneier.com/blog/archives/2005/09/fingerprint-loc.html>

Human rights

Liberty
http://www.manchesteronline.co.uk/news/s/80/80080_liberty_raps_school_fingerprint_checks.html

Privacy International
<http://www.privacyinternational.org/countries/uk/kidsprint/fingerprint-release-702.html>

The children's rights group
<http://www.arch-ed.org/fingerprinting/fingers.htm>