Data Security in iDStore

Biometric person recognition can seem to be a much scarier prospect than it really is. The aim of this document is to clearly describe the way in which Biometric fingerprint recognition is carried out and the security measures that make the storage of this information safe.

There is a very strict permissions system within iDStore allowing the parents of pupils under 18 to stop a biometric scan of their child taking place. It is a statutory requirement within England & Wales (not the rest of the UK) to have explicit permission from a pupil's parent to take a biometric scan of any kind. Beyond this, biometrics can seem intimidating when you have never come across it before. That is why it is a good idea to start communicating with parents in the early stages so that they can make an informed decision about whether or not to allow their child to be biometrically registered. If someone chooses not to use the biometric recognition side of iDStore they can still use the system with an ID card, a PIN or a password for authentication.

How Fingerprints are Handled

When someone registers their fingerprint with iDStore, their fingerprint is analysed and then converted into a series of data points by a mathematical algorithm. It is this series of data points that is stored in the iDStore database, not the fingerprint itself. This series of data points can then be used to quickly identify a person from another scan of their fingerprint. These data points cannot be used to reconstruct a useable fingerprint even with the algorithm available. The level of detail stored in these data points is well below the level of detail needed for forensic identification of someone and would be completely inadmissible, both in terms of quality and legality, in court. The data points are encrypted before being stored in the iDStore database. The encryption standard used for encrypting the data points is AES 256 with the symmetric key being stored in RSA 2048 (http://csrc.nist.gov/publications/fips/fips197/fips-197.pdf, http://www.emc.com/collateral/white-papers/h11300-pkcs-1v2-2-rsa-cryptography-standard-wp.pdf). The AES 256 encryption standard is used for storing Top Secret designated data by the American military and the NSA. Both AES and RSA are well used and commonly understood encryption standards that cannot be broken by brute force in a reasonable time.

How General Data is Stored

The iDStore database is stored within SQL Server. This is a common database engine used by a huge number of enterprise level systems. The data files cannot be read outside of SQL Server and SQL Server is always password protected. Beyond this, the fingerprint data points, as stated previously,

are stored in the database in an encrypted format. This SQL Server instance is always kept within the school. It is not stored on an internet based server or within our offices.

Common Concerns

Q: Is the data stored in iDStore safe?

A: Yes. It is stored in an instance of Microsoft's SQL Server that is on the school premises. It is not openly available over the internet or accessible outside the school network. The fingerprint data points are very strongly encrypted using military grade encryption standards.

Q: Can the encryption be broken?

A: No. The level of encryption used to store the fingerprint data points is incredibly secure and cannot be cracked using brute force in an acceptable amount of time (it would take 1 billion computers twice the age of the universe to do this).

Q: If the fingerprint data points were stolen could they be used to reconstruct the original fingerprints?

A: No. Even if the encryption could be broken, and the algorithm guessed and reverse-engineered, then the resulting image would not be recognisable as a fingerprint. It would not contain enough information to be recognised by a fingerprint scanner. It would not even contain enough information to be forensically analysed.

Q: Can the fingerprint points be used by the police to match in their database?

A: No. The algorithm used to turn the fingerprint into data points would not match another algorithm used by another system and so any other database or system that uses fingerprint recognition would not be able to use the fingerprint data points that we store.

Cunningham Cash Registers Limited
Registered in England & Wales No: 1221095
Headley Technology Park, Middle Lane, Wythall, Birmingham, B38 0DS
Tel: 01564 829999 Fax: 01564 826999