Article Title: 'The Difference Engine: Dubious security'

Origin: 'The Economist' Science and Technology 'Babbage'

Date Published: 2010-10-01

Author: N.V.

Article's Subject Matter:

The article is on Biometric technology and attempts to identify different issues of Biometrics being used for security purposes, and that it is fallible and not perfect. The writer identifies issues with technology, human errors, and cites privacy concerns with Biometrics. He/She attempts to raise concern for the use of this technology, and that reliance on Biometrics for security can have implications.

Key Points in Article

- Article attempts to bring light to issues using Biometrics for security.
- Technology issues with computerized systems identified (calibration, software/hardware limitations)
- Human errors, such as the Mayfield fingerprint case identified
- Privacy issues on collection and use of the information
- False positives, and their affect on security staff using the equipment
- The fact that biometrics can't be private, like passwords, or tokens
- Fingerprints and facial features, etc are plainly visible and not subject to privacy
- People can subvert fingerprint and other biometric devices
- States biometric systems provide 'probabilistic ' results for identity

Fallacies and Issues

- Statements on Mayfield case not completely accurate
- States that 'No one seems to be doing fundamental research on ….. , and how they change with age, disease, stress and other factors' …Obviously hadn't checked into fingerprint research
- Did not go into fingerprint identification in any great detail
- Probabilistic results for other biometrics maybe, but true fingerprint individualization – no
- If biometric systems are using probabilistic models for fingerprints….is it something that we may have to look into, as per the NAS report?

The Economist

Science and technology
Babbage

The Difference Engine: Dubious security

Oct 1st 2010, 8:22 by N.V. | LOS ANGELES

THANKS to gangster movies, cop shows and spy thrillers, people have come to think of fingerprints and other biometric means of identifying evildoers as being completely foolproof. In reality, they are not and never have been, and few engineers who design such screening tools have ever claimed them to be so. Yet the myth has persisted among the public at large and officialdom in particular. In the process, it has led—especially since the terrorist attacks of September 11th 2001—to a great deal of public money being squandered and, worse, to the fostering of a sense of security that is largely misplaced.

Authentication of a person is usually based on one of three things: something the person knows, such as a password; something physical the person possesses, like an actual key or token; or something about the person's appearance or behaviour. Biometric authentication relies on the third approach. Its advantage is that, unlike a password or a token, it can work without active input from the user. That makes it both convenient and efficient: there is nothing to carry, forget or lose.

The downside is that biometric screening can also work without the user's co-operation or even knowledge. Covert identification may be a boon when screening for terrorists or criminals, but it raises serious concerns for innocent individuals. Biometric identification can even invite violence. A motorist in Germany had a finger chopped off by thieves seeking to steal his exotic car, which used a fingerprint reader instead of a conventional door lock.

Another problem with biometrics is that the traits used for identification are not secret, but exposed for all and sundry to see. People leave fingerprints all over the place. Voices are recorded and faces photographed endlessly. Appearance and body language is captured on security cameras at every turn. Replacing misappropriated biometric traits is nowhere near as easy as issuing a replacement for a forgotten password or lost key. In addition, it is not all that difficult for impostors to subvert fingerprint readers and other biometric devices.

Biometrics have existed since almost the beginning of time. Hand-prints that accompanied cave paintings from over 30,000 years ago are thought to have been signatures. The early Egyptians used body measurements to ensure people were who they said they were. Fingerprints date back to the late 1800s. More recently, computers have been harnessed to automate the whole process of identifying people by biometric means.

Any biometric system has to solve two problems: identification ("who is this person?") and verification ("is this person who he or she claims to be?"). It identifies the subject using a "one-to-many" comparison to see whether the person in question has been enrolled in the database of stored records. It then verifies that the person is who he or she claims to be by using a "one-to-one" comparison of some measured biometric against one known to come from that particular individual.

Scanning the fibres, furrows and freckles of the iris in the eye is currently the most accurate form of biometric recognition. Unfortunately, it is also one of the most expensive. Palm-prints are cheaper and becoming increasingly popular, especially in America and Japan, where fingerprinting has been stigmatised by its association with crime. Even so, being cheap and simple, fingerprints remain one of the most popular forms of biometric recognition. But they are not necessarily the most reliable. That has left plenty of scope for abuse, as well as miscarriage of justice.

The eye-opener was the arrest of Brandon Mayfield, an American attorney practicing family law in Oregon, for the terrorist bombing of the Madrid subway in 2004 that killed 191 people. In the paranoia of the time, Mr Mayfield had become a suspect because he had married a woman of Egyptian descent and had converted to Islam. A court found the fingerprint retrieved from a bag of explosives left at the scene, which the Federal Bureau of Investigation (FBI) had "100% verified" as belonging to Mr Mayfield, to be only a partial match—and then not for the finger in question.

As it turned out, the fingerprint belonged to an Algerian national, as the Spanish authorities had insisted all along. The FBI subsequently issued an apology and paid Mr Mayfield $2m as a settlement for wrongful arrest. But in its rush to judgment, the FBI did more than anything, before or since, to discredit the use of fingerprints as a reliable means of identification.

What the Mayfield case teaches about biometrics in general is that, no matter how accurate the technology used for screening, it is only as good as the system of administrative procedures in which it is embedded. That is also one of the finding of a five-year study ("Biometric Recognition: Challenges and Opportunities" (http://www.nap.edu/openbook.php?record_id=12720&page=R1)) published on September 24th by the National Research Council in Washington, DC.

The panel of scientists, engineers and legal experts who carried out the study concludes that biometric recognition is not only "inherently fallible", but also in dire need of some fundamental research on the biological underpinnings of human distinctiveness. The FBI and the Department of Homeland Security are paying for studies of better screening methods, but no one seems to be doing fundamental research on whether the physical or behavioural characteristics such technologies seek to measure are truly reliable, and how they change with age, disease, stress and other factors. None looks stable across all situations, says the report. The fear is that, without a proper understanding of the biology of the population being screened, installing biometric devices at borders, airports, banks and public buildings is more

likely to lead to long queues, lots of false positives, and missed opportunities to catch terrorists or criminals.

What is often overlooked is that biometric systems used to regulate access of one form or another do not provide binary yes/no answers like conventional data systems. Instead, by their very nature, they generate results that are "probabilistic". That is what makes them inherently fallible. The chance of producing an error can be made small but never eliminated. Therefore, confidence in the results has to be tempered by a proper appreciation of the uncertainties in the system.

On the technical side, such uncertainties may stem from the way the sensors were calibrated during installation, or how their components degrade with age. Maybe the data get corrupted by inappropriate compression, or by bugs in the software that surface only under sporadic conditions. The sensors may be affected by humidity, temperature and lighting conditions. Effects may be aggravated by the need to achieve interoperability between different proprietary parts of the system. There are endless ways for performance to drift out of true.

On the behavioural side, uncertainties may arise from an incomplete understanding of the distinctiveness and stability of the human traits being measured. The attitude of people using the system may affect the results. So will their experience with, or training for, such scanning equipment.

Whatever, if the likelihood of an impostor or wanted criminal showing up is rare, even recognition systems that have very accurate sensors can produce a lot of false alarms. And when a system generates a fair number of false positives relative to the remote possibility of a true positive, operators will inevitably become lax. That is a fact of life. And when that happens, it defeats the whole objective of having a screening process in the first place.

The body of case law on the use of biometric technology is growing, with some recent cases asking serious questions about the admissibility of biometric evidence in court. Apart from privacy and reliability, biometric recognition raises important issues about remediation. Increasingly, we can expect the courts to use remediation as a way of addressing both lax and fraudulent use of biometrics, especially for individuals (like Mr Mayfield) who have been denied their due rights because of an incorrect match or non-match in some screening process.

The biometrics industry has a vital role to play in these threatening times. But it would win broader acceptance if it paid greater attention to the concerns and cultural values of the people being scanned. And everyone would be better served if a good deal more was known about what it is, biologically, that makes each and everyone of us a unique human being.