

The challenge of building safe and reliable of biometric systems

RISE conference, Brussels 9, December 2010

Ronald Huijgens
Unisys, Netherlands Biometric Forum



Contents

- Introduction
- Biometrics considered
- Why do we need biometrics?
- When do we need biometrics?
- The fallacy of the wrong level
- Identity Fraud
- Privacy
- Principles for safe and reliable biometric systems
- Conclusion

Introduction

- Netherlands Biometric Forum (NBF) is a foundation that promotes meaningful, safe and reliable use of biometrics:
 - Highlight the interest of both public and professionals
 - Create awareness around the risks and opportunities associated with the use of biometrics
 - Achieve social acceptance of the technology
 - Trust is the key for acceptance, and this must be earned!
 - Participants from public and private sector and academic world work together on formulation the key principles for meaningful, safe and reliable use of biometrics
 - NBF Position Paper, www.biometrieforum.nl

Biometrics considered

- We use biometrics for automated recognition of individuals based on their behavioural and biological characteristics
- Enrolment:
 - Capture and digitize behavioural and biological characteristics from an individual,
 - Register the biometric data and store it for later reference
 - Associate the biometric data to identifying information as a reference for later use, e.g. Name
- Verification
 - Capture and digitize behavioural and biological characteristics from an individual
 - Retrieve previously registered biometric data that is associated with identifier
 - Compare the two
 - This is done at another place and time as the enrolment

Biometrics considered | 2

- Biometric matching is based on laws of probability, so one can **always** expect
 - False matches
 - False non-matches
- Biometrics **never** give 100% certainty, and **can** make the wrong associations between individuals' biometric data and their ID documents or data.
- Biometrics can not make statements about integrity of ID documents and data that it uses as reference.
- Biometrics can not establish identity, it can only recognise individuals with a certain level of accuracy
- ***Conclusion: Biometrics are vulnerable to privacy and security concerns***

Why do we need biometrics?

- We live in an anonymous information society characterised by increasing global mobility
- Automated recognition of individuals is becoming increasingly important
- Traditional methods (PIN, passwords etc) are not 'personal' enough
- Biometrics will become a necessity for sensitive work processes in the public and private sectors
- Biometrics is very useful when
 - There must be a level of certainty about the person's ID
 - There must be a level of certainty that a person's ID can't be misused

When do we need biometrics?

- The requirements for automated biometric recognition of individuals will be different, depending on the context.
- Example 1: swimming pool
- Example 2: car rental
- There is no point in storing biometric data when
 - This does not help solve the issue at hand
 - Data is or has become useless, obsolete or unreliable

When do we need biometrics?

- Observations from the examples:
 - It is easy to build a system whose biometric data can be misused.
 - Providing information to the public and organisations who plan to use biometrics.
 - It is vital to protect biometric data, certainly those which are derived from unalterable biometric characteristics such as fingerprints.
 - Once biometric data is compromised, the problem will remain for a long time without the possibility of defending ourselves by altering that biometric characteristic.

The fallacy of the wrong level

- Most current biometric applications are for relatively small groups of people, with a certain level of control
- The experience coming from these small-scale systems related to behaviour and dynamics are easily copied to large-scale systems of a chain or a sector.
- This is called the ‘fallacy of the wrong level’
- Example 3: [ePassport](#)
 - Small scale: 1:1 verification fingerprint is reliable
 - Large scale: huge numbers of stakeholders heavily decrease manageability
- Example 4: [EU Visa](#)
 - Checks against the database can provide criminal organisations with operational information

Identity Fraud

- Identity fraud can be defined as a person who maliciously and deliberately creates the suggestion of an identity that is not his/her own.
- The ID of another person is misused or a non-existing identity is created.
- **Any** identifier can be used, Citizen ID number, photo biometric, as they all contain a **suggestion** that people believe.
- ID fraud proves to be easy and has low risk
- At identity checks, hardly any verification details other than those held by the person are being checked
- Chance of getting caught is small !!!

Identify fraud | 2

- Travel- and ID documents (ID cards etc) , citizen service number or biometric details are of extra value to identity fraudsters because they must and can be used everywhere!
- In official verification systems, the process is very predictable
- Fallback scenarios are generally weak, and can be initiated by the fraudsters themselves
- ID fraud leaves traces in the (digital) world
- If the ID fraud was successful, all traces point to the victim
- The victim has to prove that he/she has **not** done something

Identity fraud | 3

- Can biometrics help prevent ID fraud?
- Safety assessment:
 - Can the ID check be fooled by imitating the biometric of the holder?
 - Can the ID check be influenced from external sources?
 - Can the ID check results be obtained and misused?
- This applies to the entire, end-to-end solution
- Unsafe biometric applications are a threat to citizen privacy
- Prevention of identity fraud is an important reason for using biometrics

Privacy

- ID fraud leaves traces that lead to the victim
- ID Fraud implies a very serious violation of the victim's privacy
- Specifically when an unalterable biometric feature is compromised (e.g. fingerprint)
- The compromised biometric traces (e.g. at a crime scene) lead to the victim, this is very hard to deny.
- ID fraud is very difficult, expensive and time consuming to solve

Protecting biometric data

- Provisions to verify the integrity of biometric data should be taken.
 - Multiple biometric features are to be used to enable detection of malicious use of identities. Separate biometric features can be used, provided that they remain within their own domain
 - Multifactor authentication
 - Encryption, signing and access control can help achieve that
- Misuse (for purposes for what it was not intended) of biometric data must be prevented
 - PKI
 - Privacy Enhancing Technologies
- Application Logic must provide this

Principles for safe and reliable biometric systems

- Biometrics are not conclusive.
- Biometrics can only recognise people, it cannot establish identities
- Safety assessments are absolutely necessary to safe and reliable large-scale biometrics applications.
- The principle of "*at least three matches*"
- Actively discourage the trivial use of biometrics
- It should be practically impossible to re-use biometric data in other applications than what it is intended for.
- Large-scale biometrics applications should be registered, certified and monitored

Principles for safe and reliable biometric systems | 2

- Biometric verification must meet number of requirements
 - Biometrics is bound to its intended purpose
 - Simple procedures for objections and complaints are established
 - Fallback procedure is proportionate to the risks involved
 - Preventative measures against theft or misuse of biometric data
 - Active management by the operator (compensation for damages and rehabilitation)
 - Transparency on access to biometric data
 - Explicit measures against fraudsters who (try to) biometric data
- The storage of biometric data should only be permitted if essential to the application in question.
- Linking biometric data to external databases must be legally mandated, with no link to other personal data

Conclusion

- Building biometric applications is complex
- Large scale biometrics systems need to be carefully implemented
- Next to normal systems, increased complexity due to
 - Protection of biometric data
 - Fall-back scenarios
 - Restricting the use of biometric to its intended purpose
 - Provisions to be able to check data integrity
 - Biometrics can not be used on its own
 - Procedures for complaints and corrections
- Legislation needs to be adopted and respected to guarantee safe and reliable biometrics
- Transparency is essential, especially for large scale systems the public must be timely and fully informed
- Do not use biometrics when it is not necessary

Thank you

- Questions?

Ronald Huijgens
Director Biometric Technologies
TCIS, WW Client Engagement Team

UNISYS
imagine it. done.

Unisys Nederland N.V.
Tupolevlaan 1
1119 NW Schiphol-Rijk
The Netherlands

+31 20 526 7500
+31 20 526 7700 Fax
+31 6 1000 1543 Mobile
ronald.huijgens@nl.unisys.com

UNISYS

imagine it. done.

Sidestep slides

Example 1

(source: Prof. Dr. mr J.H.A.M.Grijpink)

A swimming pool wanted to use fingerprint verification to exclude a certain group of boys that was repeatedly harassing girls.

All visitors (both male and female) were asked to register their fingerprints in the swimming pool's computer system at each visit.

This application threatens the bright future of biometrics.

If you have the fingerprints of the boys you want to exclude from swimming, it is sufficient to check the fingerprints of male visitors belonging to the relevant age group. Second, if someone's fingerprint is included in the blacklist, he can be sent on his way

There is no point whatsoever in checking and storing the fingerprints of girls. A woman of 82 refuses to cooperate with having her fingerprints checked and is therefore banned from the swimming pool.

Such a blacklist may be constructed and maintained under the European Data Protection Directive and Dutch national law if the culprit's fingerprints are taken after a case of misbehaviour and used during a limited period of time and if the list's purpose is clearly explained to the public and the boys involved.

Example 2

(source: Prof. Dr. mr J.H.A.M.Grijpink)

A car rental company was having a lot of difficulties with cars being returned. Many rented cars were not returned or were taken to the wrong place. Biometrics looked promising, but must not be too expensive.

A creative employee came up with a solution without the need for expensive electronics: the fingerprint was placed on the paper rental contract with gel, with the assurance that the paper containing the fingerprint would be returned when the car was brought back.

This experiment proved to be a resounding success: during the experiment no stolen or incorrectly returned vehicles!

All well and good. But watch out!

This simple biometrics system was introduced elsewhere by the same company, too. A few months later this site's administration proved to be full of copies of rental contracts with fingerprints without there being any need for them!

Example 3

(source: Prof. Dr. mr J.H.A.M.Grijpink)

Our first example concerns the new biometric passport. This is based on the notion that somebody can accurately be verified by his fingerprint.

This essentially small-scale notion should not automatically be extended to the national or international scale of border control. Otherwise it is uncertain whether the biometric passport delivers what is expected of it.

Large-scale systems function differently from small-scale ones because on this scale there is no coordinating or enforcing authority. Moreover, large-scale systems involve huge numbers of stakeholders (members of the public, travellers and patients) and cooperating autonomous organisations and professionals that causes large-scale processes to be barely manageable. Despite all good intentions much goes wrong.

Biometrics, too, can be supposed to work differently at large-scale level (chain, sector, country) than one might think from small-scale ideas, and can sometimes be counter-productive. Imitating or counterfeiting the fingerprint on the passport can enable someone to get through the check without it being possible to find out afterwards who it was because traces left inherently point to the official holder, not to the identity fraudster.

Example 4

(source: Prof. Dr. mr J.H.A.M.Grijpink)

The biometric visa, has already been introduced to keep out unwanted foreigners even before they come to the Netherlands. For that reason the fingerprints of the traveller are taken at the Dutch embassy in the country of origin during the visa application and sent to the Netherlands. If those fingerprints are included in the database of fingerprints of unwanted foreigners, the visa is refused.

Biometrics can in some cases be counterproductive at that large-scale level.

Take a situation where a criminal network wants to send someone to the Netherlands for a criminal act. If the visa is refused, the network knows that it will either have to send someone else or choose a route where the checks are less well organised. That means that rather than the anticipated tighter grip on incoming passenger traffic, the target group of unwanted foreigners can imperceptibly become invisible!

Generic biometric system architecture

