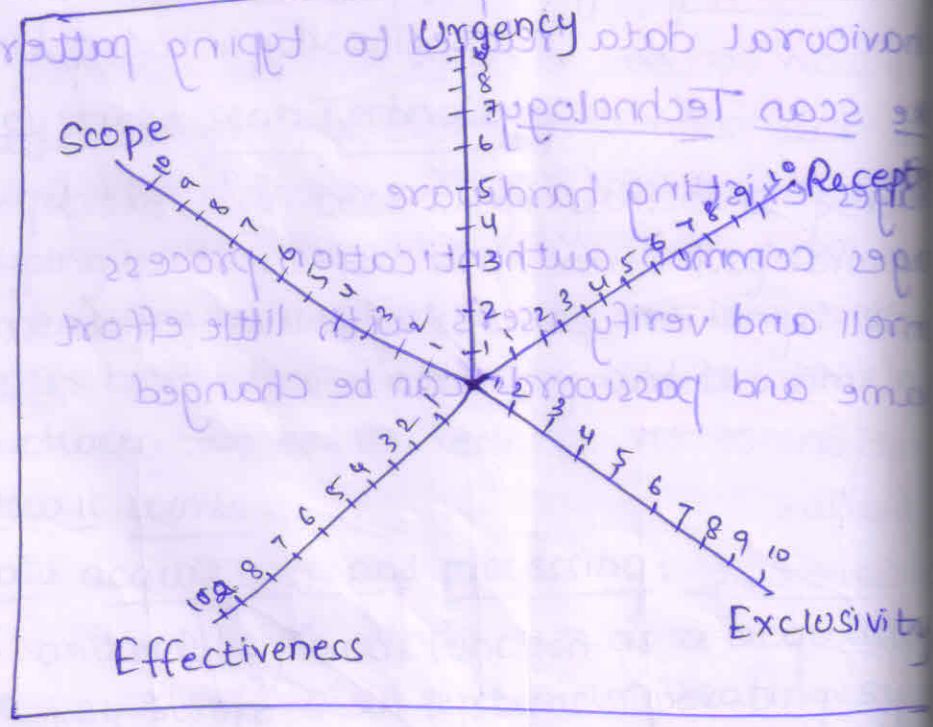
UNIT-IV

BIOMETRIC APPLICATIONS

Biometric solution matrix:

The biometric solution matrix is a guide biometrics for specific applications, desig help deployers assess the nature of their authentication problem. The biometric solu defines the five elements that deployers consider when deciding whether to imp biometrics

1. Urgency
2. Scope
3. Effectiveness
4. Exclusivity
5. Receptiveness



1) How urgent is the authentication problem that biometrics are solving?

An authentication problem may be deemed urgent as a result of substantial risk of valuable data, assets, revenues or public safety. Biometric deployments become more important to an institution when the authentication problem they must solve is urgent

In the biometric solution matrix, urgency is rated on a scale of 1 to 10

---

2) What is the scope of the authentication problem that biometrics are solving?

Biometrics can be used to address an authentication problem that is limited in scope, such that only a small percentage of individuals might interact with the biometric system or to address authentication problems encountered by a large number of individuals on a regular basis

Biometrics are more likely to be a strong solution when addressing authentication problems that are broad in scope. Scope is rated on a scale of 1 to 10

---

3) How well (effectiveness) can biometrics solve the authentication problems?

Biometrics are more valuable to deployers when the methods are used, are highly capable of effectively solving authentication problems

In the biometric solution matrix, effectiveness is rated on a scale of 1 to 10

4) ~~Are~~ biometrics the only possible authe solution?

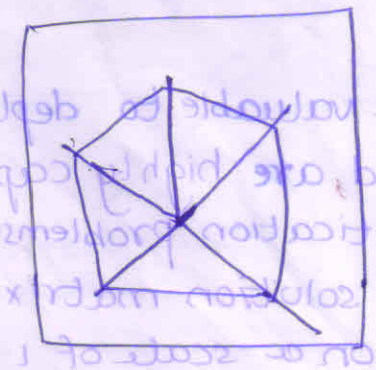
Biometrics might be the only solution authentication problem or one of many solutions. Biometrics are stronger solutio applications in which they are the on alternative to an authentication prob

Exclusivity is rated on a scale of 1 to

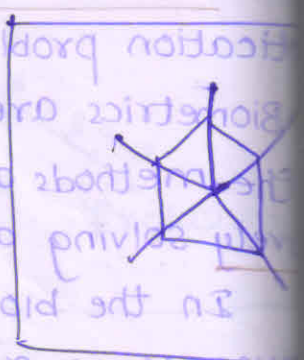
5) How receptive are users to biometrics as authentication solution?

Biometrics might be welcomed necessary authentication solution or the dismissed as a possible solution for a ve reasons. Without receptiveness informed by employees and citizens, the potential for b to be an authentication solution is limite Receptiveness is rated on a scale of 1 to 10

By plotting the five elements of the biom solution matrix, potential deployers can ass suitability of biometric technology for the particular application.



Strong solution



Weak solut

Bioprivacy Technology Risk Ratings:

Each type of biometric deployment can have a different impact on privacy

The bioprivacy technology risk ratings assess the privacy risks of leading biometrics technologies, defining which technologies require more explicit system-design productions than others

The technology risk ratings evaluate biometric technologies according to 3 categories presented in the input framework

1- Verification / Identification
2- Overt / Covert
3- Behavioural / Physiological

The technology risk ratings include a 4th category referred to as Give / Grab

Biometric systems can acquire biometric data in two ways

1- When an individual gives biometric data at the time of his/her choosing after initiating an enrollment or verification sequence
2- When the biometric system grabs biometric data without the user having initiated an enrollment or verification system
3 Each technology is given a Risk Rating of low, medium or High

Verification / Identification:

Technologies only capable of verification are rated lower. Technologies capable of robust identification are rated higher

Overt/Covert:

Technologies requiring the individuals be biometric system operation are rated lower Technologies capable of operating without or consent are rated higher

Behavioural/Physiological:

Technologies based on variable behaviou are rated lower. Technologies based on physiological characterstics are rated high

Give/Grab:

Technologies in which the user gives biome rated lower

Techologies in which the system grabs without the user initiating a sequence are higher

Low: Little if any privacy risks

Moderate: Limited privacy risks

High: Substantial privacy risks

Technology risk ratings

Technology	positive privacy aspects	Negative privacy aspects	Bioprivacy Technology Risk ratings
Fingerscan	• Large variety of vendors with different templates and algorithms • Can provide off fingers for diff systems changes in hair style, facial hair, position, lighting reduce ability of technology to identify individuals	• use on forensic applications • storage of images in public sector applications • strong identification capabilities	• Verification / Identification: H • Overt/covert: M • Behavioural/ Physiological: H • Give/Grab: M Risk Rating: H
Facial scan		• easily captured without consent or knowledge • existing facial image database can be used for comparison	• verification/ identification: H • overt/covert: H • Behavioural/ Physiological: M • Give/Grab: H • Risk Rating: H
Iris scan	• Requires high degree of user cooperation difficult to acquire without consent • Require properitary acquisition device • Not used in forensic application	• very strong identification capabilities • development of technology may lead to covert acquisition capability • only one type of iris template no vendor heterginity	• verification/ Identification: H • Overt/covert: L • Behavioural/ Physiological: H • Give/Grab: M • Risk Rating: M
Retinascan	• Require high degree of user cooperation cannot be captured without consent • Requires properitary acquisition device	• very strong identification • Indicate certain eye deseases	• verification/ Identification: H • Overt/covert: L • Behavioural/ Physiological: H • Give/Grab: L • Risk Rating: M

Voice Scan	• voice is text dependent • not capable of identification	• Biometric data can be captured without consent	• Verification/ Identification • Overt/Covert • Behavioural/ Physiological • Give/Grab: M • Risk Rating: M
Signature Scan	• signing is largely behavioural	• can be used to commit fraud	• Verification/ Identification • Overt/Covert: + • Behavioural/ Physiological • Give/Grab: M • Risk Rating: L
Keystroke Scan	• A highly behavioural characteristic	can be captured without consent	• verification/ Identification • Overt/Covert: L • Behavioural/ Physiological • Give/Grab: L • Risk Rating: L
Hand Scan	• physiological biometric but not capable of identification • Require properitary device • Not a palm scanner but a measure of hand structure	None	• Verification/ Identification • Overt/Covert: L • Behavioural/ Physiological • Give/Grab: L • Risk Rating: L

* It would be a mistake to conclude from the technology Risk Rating that finger scan and facial scan deployments should be limited and that lower risk technologies are preferable.
* Factors such as accuracy, price, process flow, ease of integration into current systems, from factors and existing authentication schemes normally drive deploym

Designing p

Bioprivacy

The first
design is t
capabilitie
and how

I Limit Su

1.) It is di
categorica
its original
transperan
be more
governmen
and priva

2) Do not
3) Limit
4) Evaluate
5) Limit
6) Limit
informa
7) Make

II Data Prote

1) Use rec
protect b
2) Protect
3) Limit
4) Implem
between

Recruit

Designing privacy sympathetic biometric systems:

Bioprivacy Best practices: scope and capabilities:

The first challenge of privacy - sympathetic system design is to address the systems scope and capabilities what the system is meant to do and how it accomplishes the task

I) Limit System scope:

1) It is difficult to design a system that categorically cannot be used for purposes beyond its original intent, auditing, overright and transperancy are essential scope limitation may be more difficult in countries with authorization governments, where frame works to ensure public and private actor accountabilities may be looking
2) Do not use biometrics as a unique identifier
3) Limit retention of biometric information
4) Evaluate a system's potential capabilities
5) Limit storage at identifiable biometric data
6) Limit collectional storage of extra rises information
7) Make provision for system termination.

II Data Protection:

1) Use recruits tools and a access policies to protect biometric information
2) Protect port match decision
3) Limit system access
4) Implement logical and physical representation between biometrics and non-biometric data

III. User Control of personal data:

1) Make system usage voluntary and allow for unenrollment
2) Enable an any rows enrollment and verification
3) Provide means of correcting and accesing biometric related information

IV Disclosure, auditing and Accountability:

1) Make provisions for third-party auditing and overnight
2) Hold operation account able for system use and reuse
3) Fully disclose audit findings
4) Disclose the system purpose and objectives
5) Disclose when individuals may be enrolled in a biometric system
6) Disclose when individuals may be verified in a biometric system
7) Disclose whether enrollment is optional or mandatory
8) Disclose enrollment, verification and identification process
9) Disclose policies and protection in place to ensure privacy of biometric information

BIOMETRIC STANDARDS:

The lack of industry wide standards has delayed many types of biometric implementation and has slowed the growth of biometric industry.

The only segment of the biometric industry with mature and widely adopted standards is live scan fingerprint imaging, driven by urgent

of law enforcement agencies. In the absence of biometric standards is said to be immature or developmental. standardization is taken as a sign of technology's maturity

The biometric industry is actively addressing the standards problem, with some key efforts finalized and the process of industry adoption underway

Completed and ongoing standard efforts address a range of technical areas: application programming interface, file formats, encryption, image capture and data exchange

Why standards?

At this stage in development, large majority of biometric systems both hardware and software in many respects:

→ the manner in which biometric devices and systems communicate with applications
→ the method by which features are extracted from a biometric sample
→ the method by which biometric data is compared
→ the length and content of biometric templates including reader data and methods of encryption
→ the method by which biometric data is stored and retreived

Standards ensure that in the future biometic technology will be developed and deployed in accordance with generally accepted principles of information technology

API :

Application Program Interface (API) standards ensure that developers can address a whole range of biometric technologies and devices in a standardized fashion

The development of biometric API has been a long and continuous process, marked by competing efforts, merges, alliances and major licensing agreements

BIOAPI

The BIOAPI construction has been one of most prominant standard efforts since its inception in April 1988

BIOAPI is concerned with standardizing the usage applications communicate with biometric devi and the way the data is manipulated and sto This would allow companies that deploy BIOAPI compliant technologies to change device without having to rewrite their software, BIOAPI does this by giving applications developers a comm set of function calls for biometric devices. BIOA is attempting to create modular access to biometric functions, algorithms and devices a framework allowing programers to developer a biometric devices then easily makes them work compatible with other devices

BAPI :

From April 1999 to May 2000, BIOAPI was the primary biometric API effort with dozens of biometric vendors joining its developing effort

A biometric effort reffered to as BAPI - which predated BIOAPI was merged with BIOAPI, and formed the basis of same of BIOAPI's underlying element was liscensed by microsoft in may 2000 for incorporation for the future versions of OS

Inclusion of biometric as a core component of a microsoft OS has helped legitimate the biometric industry - shifting the perception of biometrics from that of a futuristic biometric functionality in the OS means that the OS will be capable of communicating with biometric devices in standardized way. The OS communicates with priaters, configuration and setup were adours process, now printer installation is greatly simplified required only driver installation

Is DNA a BIOMETRIC?

→ In current state, DNA matching varies from standard biometrics in different ways

→ DNA requires a tangible physical sample as opposed to an image, recording or impression of a behavioural or physiological characterstics

→ DNA matching is not done in real time and currently not all stages of comparison are automated

→ DNA matching does not employ templates or feature extraction, but rather represents the comparison of actual samples

Basically fingerprints are scanned and the templates are matched. The matching is done using templates. DNA cannot be matched with the biometrics. We should take the samples and the

samples are used for verification. Automation of DNA in all aspects are not upto the mark at present.

The discussion on how, when and where DNA should and should not be used, who will control the data and how it should be stored is necessary. The conditions under which its use, collection, storage and disposal are acceptable must be defined and enforced

→ Identification samples of DNA is different for public sector

→ It cannot be used as same biometric for criminal technology

→ It is powerful tool for determining innocence or guilt. It is used in different range of applications So, it is called as a powerful tool

→ The DNA can also be used for misusage of personal information

→ It becomes uncertain to determine whether DNA can be considered as a biometric or not?

BIOMETRIC MIDDLEWARE:

A software should be designed to enable any biometric device so broader solution, known as biometric middleware, it is also widely used in marketplace.

Biometric middleware is an authentication software that

1. Enables various biometric devices and technologies

2. Allows the match or no-match decisions made by core technologies to provide authentication to various PC application and resource.

3.) It may be compatible for 5 as few and as many as 25 different authentication solutions.

4.) Middleware solutions can be seen as platforms or infrastructure that reduce dependence on a single type of biometric hardware

5.) The basic rationale behind biometric middleware is that enterprises, software developers and merchants want to integrate biometric functionality into their daily operations, products or services but do not want to be tied to a specific biometric device, solution or technology.

6.) Currently, almost all middleware solutions are deployed in employee-facing enterprise implementation over time.

7.) It is expected that middleware will play a large role in customer facing applications.

8.) it is nearly certain that home users will have access to a variety of competing hardware solutions - finger scan, voice scan, iris scan and ~~SCAN~~ and merchants will be interested in enabling these solutions.

9.) Middleware of some type will be required to bridge the gap between the end user and the merchants

10.) The competing middleware offerings which ~~each~~ need to focus less on PC/network access and ~~more on customer facing and~~ more on customer-facing and transactional applications of their software