UNIT-IV

RECOMMENDED BIOMETRIC FOR NETWORK SECURITY

* Characterstics of a good Biometric for Network Security:

→ User willingly accept the biometric device
→ Users find it easy to use
→ Total technology costs and benefits provide a suitable ROI
→ Technology is deployable and supportable
→ Technology is not invasive and requires the user to actively submit to its use
→ Technology is mature and reliable
→ Users become habituated quickly to the device

* For the biometric examined, a score of 0 to 10 was assaigned for each characterstic. An ideal biometic was defined as having a perfect score of 10 in each category.

* Finger Biometrics: →

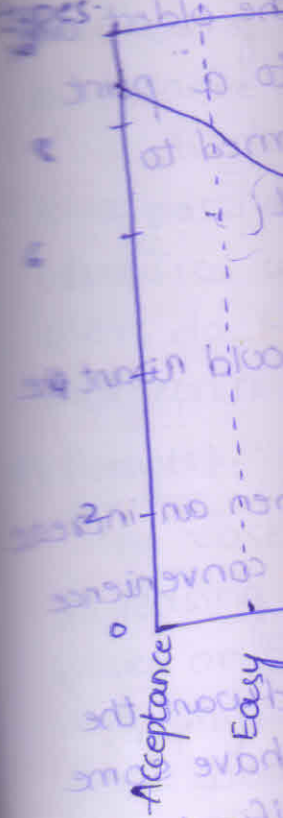
→ Its greatest strengths are deployability and maturity
→ Its greatest weakness are cost and ROI

1) Acceptance (9):

Finger biometrics are some of the oldest methods of biometric identification. People accept them because of their long history. It does not qualify for ideal status because some people feel that using their fingerprint is very similar to being fingerprinted for a criminal offence

(8-5)

ease of use
ly. The ne
ease in eas
It does n
ces may n
others ma



3) ROI (7)

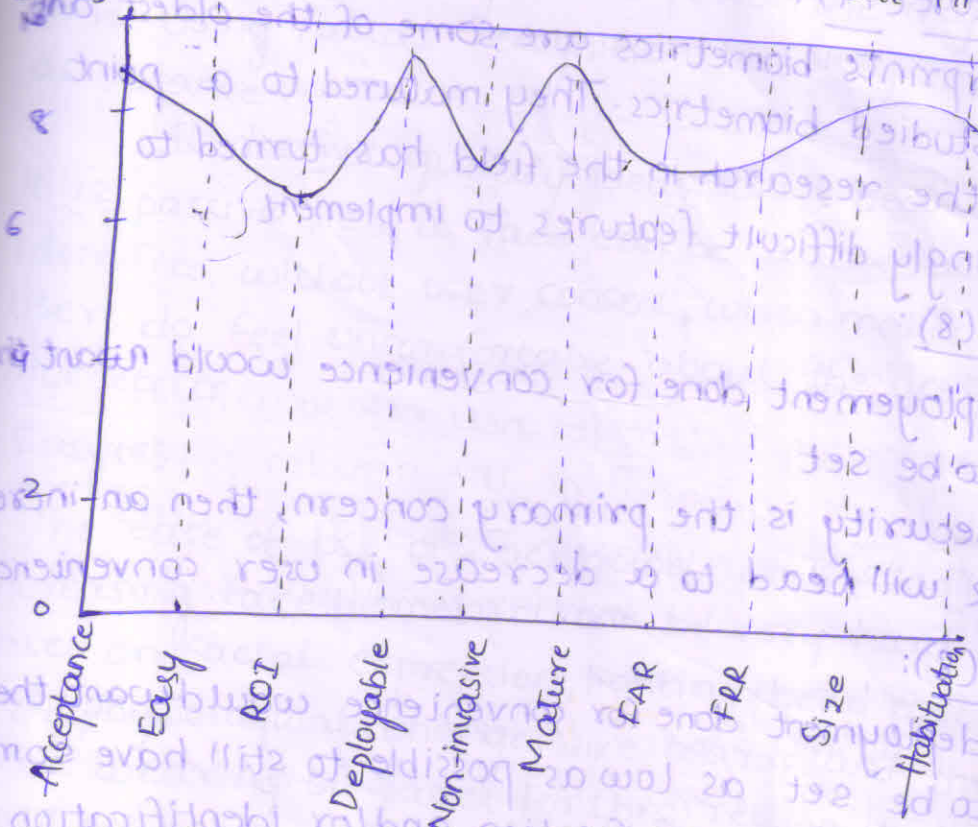
* The decr
and trainin
* It does
savings a
attracti

4) Deployab
Depl
on a de
security

2) Easy (8.5)

The ease of use of finger biometrics has increased greatly. The new sensors available have led to this increase in ease of use.

It does not qualify ideal status because some devices may not be optimal for use with all fingers and others may not work well with all finger types.



3) ROI (7)

* The decreasing cost of devices and ease of deployment and training make this a very cost effective technology
* It does not qualify ideal status because the savings alone on password - resets present a very attractive Return on Investment

4) Deployable (9.9):

Deployability considers how easy it is to get a device on a desktop. Finger biometric devices for network security have become much smaller

5) Noninvasive (8):

Since finger biometrics are associated with active devices, and they image only an exterior feature. A higher score was not given since many feel that fingerprints are very private due to the fact that they are used by law enforcement.

6) Mature (99):

Fingerprints biometrics are some of the oldest and most studied biometrics. They matured to a point where the research in the field has turned to increasingly difficult features to implement

7) FAR (8):

A deployement done for convenience would want the FAR to be set

If security is the primary concern, then an increase in FAR will lead to a decrease in user convenience

8) FRR (8):

A deployment done for convenience would want the FRR to be set as low as possible to still have some confidence in the verification and/or identification taking place

9) Size (9):

Through good design and maturity, this device has significantly reduced its physical footprint on the desktop.

10) Habituation (8.5):

A user can become habituated to a fingerprint biometric rather quickly. The placing of a finger on a scanner is relatively straight forward, but it still requires a bit of coordination

* Face Biometrics

* Its greatest s
user acceptance
* Its weakness

Acceptance (8.5)

Face biometrics
that is used to
time. Using fac
acceptance

It does n
It is passive i.e
identified with
users do feel
biometrics

Easy (6):

The ease of
increasing. Face
based on facial
and physiologic
time wearing
score well

ROI (5.5):

While it is po
technology for fa
camera should
pictures. Additi
light may be

These
specialized ca
camera deploy
period of time

* Face Biometrics :→2

* Its greatest strengths are its non-invasiveness and user acceptance

* Its weakness is ROI characterstics

1) Acceptance (8-5):

Face biometrics are natural to use. It is the face that is used to recognize a person the majority of time. Using facial recognition has very wide acceptance

It does not qualify ideal status because that it is passive i.e., a face can be authenticated or identified without user consent, which makes some users do feel uncomfortable about the use of face biometrics

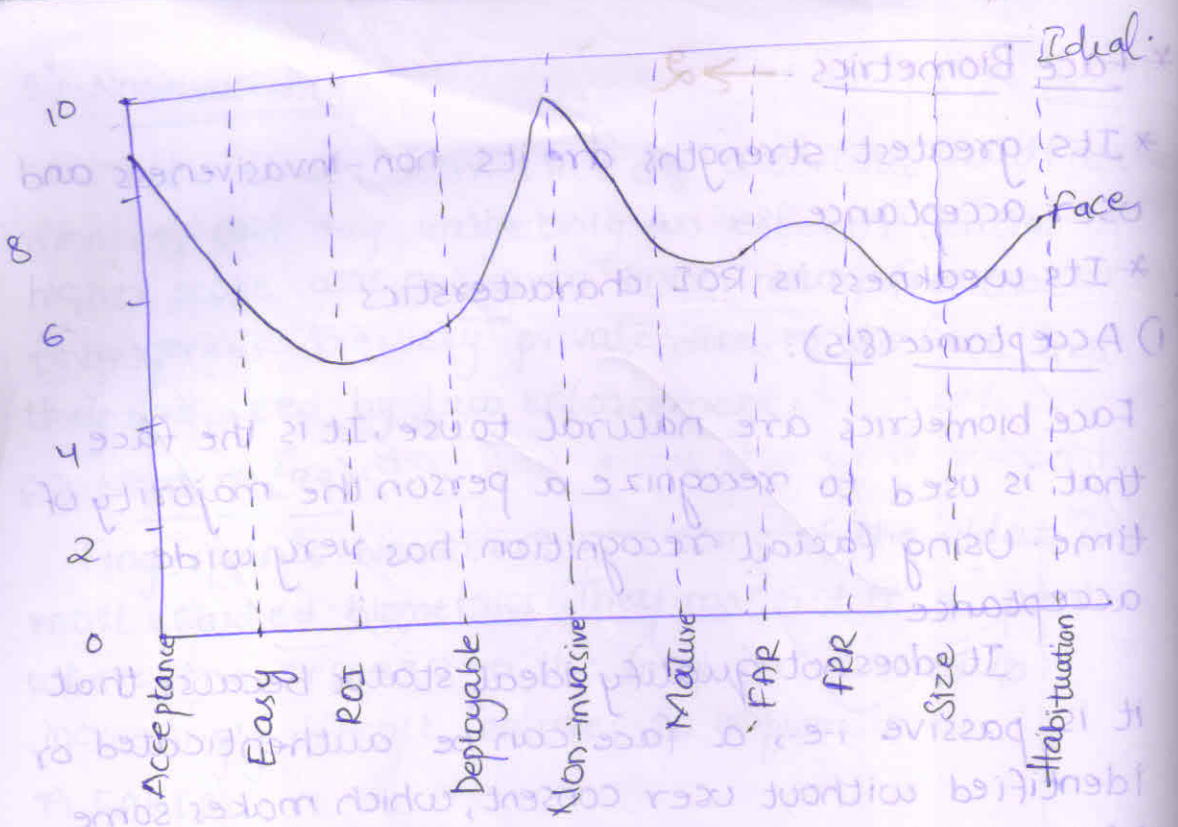
2) Easy (6):

The ease of use of face biometrics is steadily increasing. Face biometrics can be very hard to use based on facial expression, lighting, head positioning and physiological changes like beards and the part time wearing of glasses. For this reason, it did not score well

3) ROI (5-5) :

While it is possible to use of the shelf camera technology for facial recognition, a more specialized camera should be used to get the high quality pictures. Additional lighting or changes to existing light may be required.

These factors add special costs to the specialized camera, plus to the labor to get the camera deployed and functioning. This produces a larger period of time to obtain good ROI



4) Deployable (6):

Face biometric system for network security can be difficult to deploy. Based on the need for positioning the camera to capture maximum field of view, plus adjusting for possible lighting conditions, it could be a time consuming process

The time needed for deployment and the other adjustments that may be needed to make this technology more difficult to deploy

5) Non invasive (9):

Since face biometrics are so natural, users find them non-invasive. We are all comfortable with our face being used for recognition. A perfect score was not given since some may feel that face biometrics can be used as a passive tracking system

One way to increase acceptance to almost 100% is through use of a privacy-positive biometric policy

6) Mature (7)

Any picture ready source for face biom majority of biometrics, network ac needs add

7) FAR (7.5):

Face biomet other biomet low as possi increasing F

8) FRR (7.5):

With the fac to be low e the FRR. In his/her face

9) Size (6):

The size of can be large conferencing will have the requires the

Habituatio

The user ma proper angle, hold relative difficult, and habituated

6) Mature (7):

Any picture drawn or taken of the face provides a ready source for identification. The current trend for face biometrics is more for access control. As majority of biometric reasearch is done in face biometrics, less research is being done for using network access. Therefore face biometric area needs additional maturity

7) FAR (7.5):

Face biometrics also have a higher spoofing factor than other biometrics. This leads to increasing the FAR as low as possible, which then has the effect of increasing FRR

8) FRR (7.5):

With the fact that the FAR for face biometrics needs to be low enough to prevent spoofing, it will increase the FRR. In addition, the need for user to present his/her face in just right way will also increase

9) Size (6):

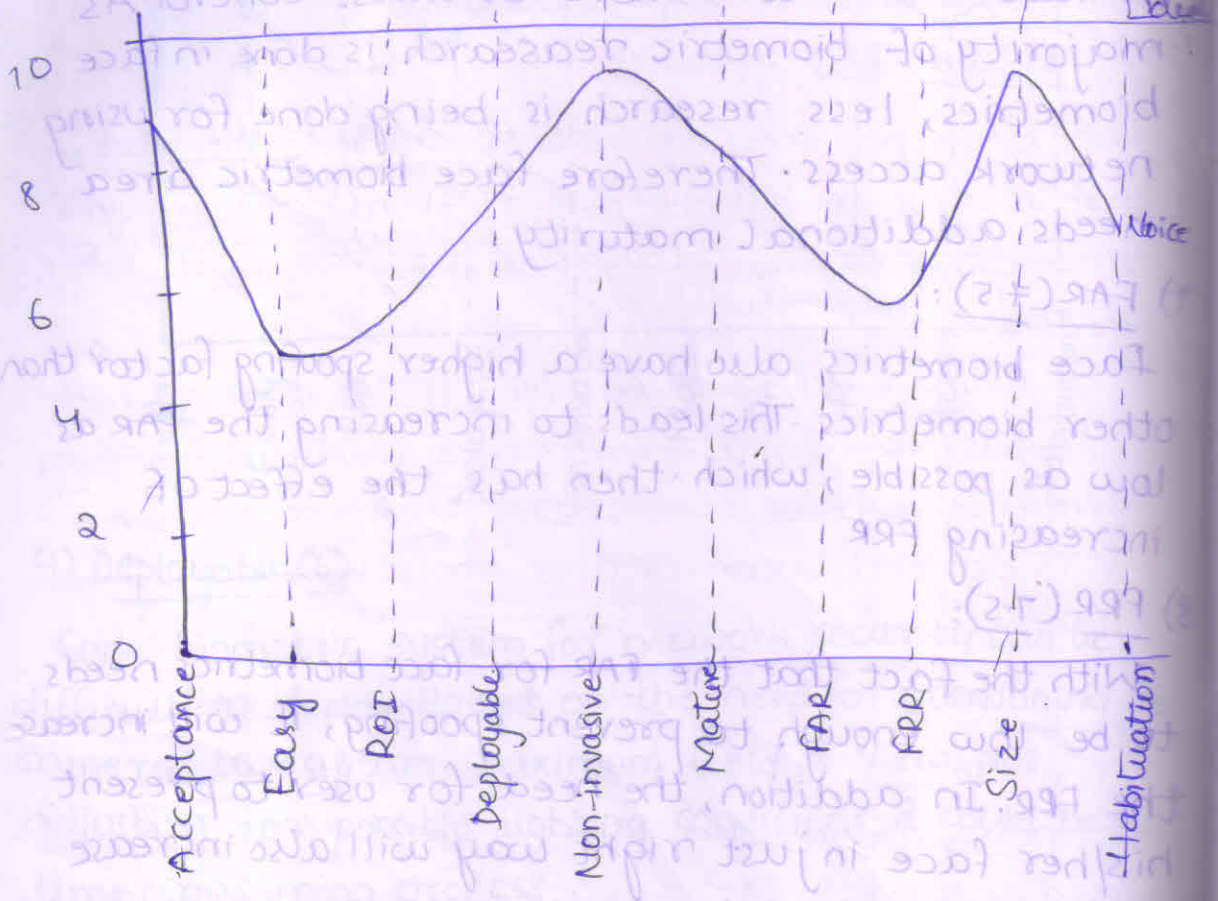
The size of specialized camera for face biometrics can be larger than a normal desktop vedio conferencing camera. Quite often, these cameras will have their own additional illumination, which requires them to be larger

10. Habituation (7.5):

The user may need to present his/her face at a proper angle, with the right neutral expression and hold relatively still. These requirements can be difficult, and so the time needed to become highly habituated could be fairly long

Voice Biometrics → 3

* Its greatest strength is size and non-invasiveness
* Its greatest weakness are FAR and FRR



1. Acceptance (8-5):

Voice biometrics rely on the user's speaking for recogni
It has wide acceptance It does not get ideal score because fact that it is passive

2. Easy (5):

The required time to train a system and enroll, coupled with the need for clear speech and low ambient noise, can make voice biometrics difficult to use

3. ROI (5-5):

The cost of hardware to use with voice biometr relatively low. A decent quality microphone is

relatively aff
is normally l
Voice Bio
enroll. They a
noise and ch
4. Deployable (8
It is relati
only to be pl
machine. Once
tested and
background n
5. Non-invasiv
We are all
recognition.
some may fe
as passive tr
acceptance t
privacy-posit
6. Mature (7):
The use of
new and still
it to mature
7. FAR (6):
For any biom
between secu
the algorithm
susceptible to
8. FRR (5-5):
For voice bi
voice changes
to hour depe

relatively affordable. The cost of deploying microphone is normally low.

Voice Biometrics can take a long time to train and enroll. They are also very susceptible to background noise and changes in the user's voice

4. Deployable (8):

It is relatively easy to deploy. A microphone needs only to be plugged into the sound card of the user's machine. Once microphone is deployed, it needs to be tested and possibly re-adjusted to minimize background noise

5. Non-invasive (9):

We are all comfortable with using our voice for recognition. A perfect score was not given since some may feel that voice biometrics can be used as passive tracking system. One way to increase acceptance to almost 100% is through the use of privacy-positive-biometric policy

6. Mature (7):

The use of machines of voice biometrics is relatively new and still additional research and time for it to mature

7. FAR (6):

For any biometric, you must decide on the tradeoff between security and user convenience based on the algorithm. The voice biometrics is also fairly susceptible to spoofing attacks

8. FRR (5.5):

For voice biometrics, there can be a very high FRR. The voice changes over time and can also vary from hour to hour depending on physical health and ambient

environment. The enrollment procedure can also lead to an increased FRR

9. Size (9.9):
The size of microphone is very small and will use almost minimal real estate on desktop

10. Habituation (7.5):
The user needs to present his/her voice at a right pitch, tempo, cadence. Those things can be difficult for people to do, so the time needed to be come habituated to the degree required could be relatively long

Iris Biometrics: → 4
* Its greatest strengths are FRR and FAR
* Its greatest weakness is high invasive

1. Acceptance (4):
Even though iris biometrics have high cool factor, users are less accepting them. Users have a hard time coming to grips with a light being shined into their eyes. It is fear of injury to the eye that increases their uneasiness

2. Easy (4):
As the biometric in use is actually internal to the body the positioning and relative closeness of the user to the reader are very-high. Also the need to perfectly align the eye with scanner is required

3. ROI (4.5):
The cost of hardware needed for iris biometrics is relatively high. The camera needs to have a specialized light source to properly illuminate

4. Deployable (6)
An iris biome
similar to the
biometric cam
lighting condit
spend time fi

5. Noninvasive
The iris bio
noted that
are invasive is
be changed
wide spread

6. Matore (6)
The reason
and strength
high maturi
additional

FAR (9):
It is very r
of comparison
was seen.

3. FRR (7.5):
The majorit
error in place
difficulty in
score. These

Size (6):
The size of
is relatively
desktop real

4. Deployable (6):

An iris biometric camera for network security is similar to the face biometric for deployment. An iris biometric camera is not susceptible to ambient lighting conditions. This can require installer to spend time fine-tuning the camera for each user

5. Noninvasive (1):

The iris biometrics are most invasive. It should be noted that most of the insistence that iris biometrics are invasive is purely user perception. Perception can be changed over time with education and more wide spread use

6. Matore (6):

The reason behind the use of iris and the simplicity and strength of the algorithm, lead to a relatively high maturity score. Where the iris biometric needs additional maturity in areas like user acceptance

7. FAR (9):

It is very robust and reliable. In the tens of millions of comparisons done in testing, not one false acceptance was seen.

8. FRR (7.5):

The majority of FRR is normally caused by user error in placement of the iris for recognition. This difficulty in placement is what drives down the score. These failures are also called 'failures to acquire'

9. Size (6):

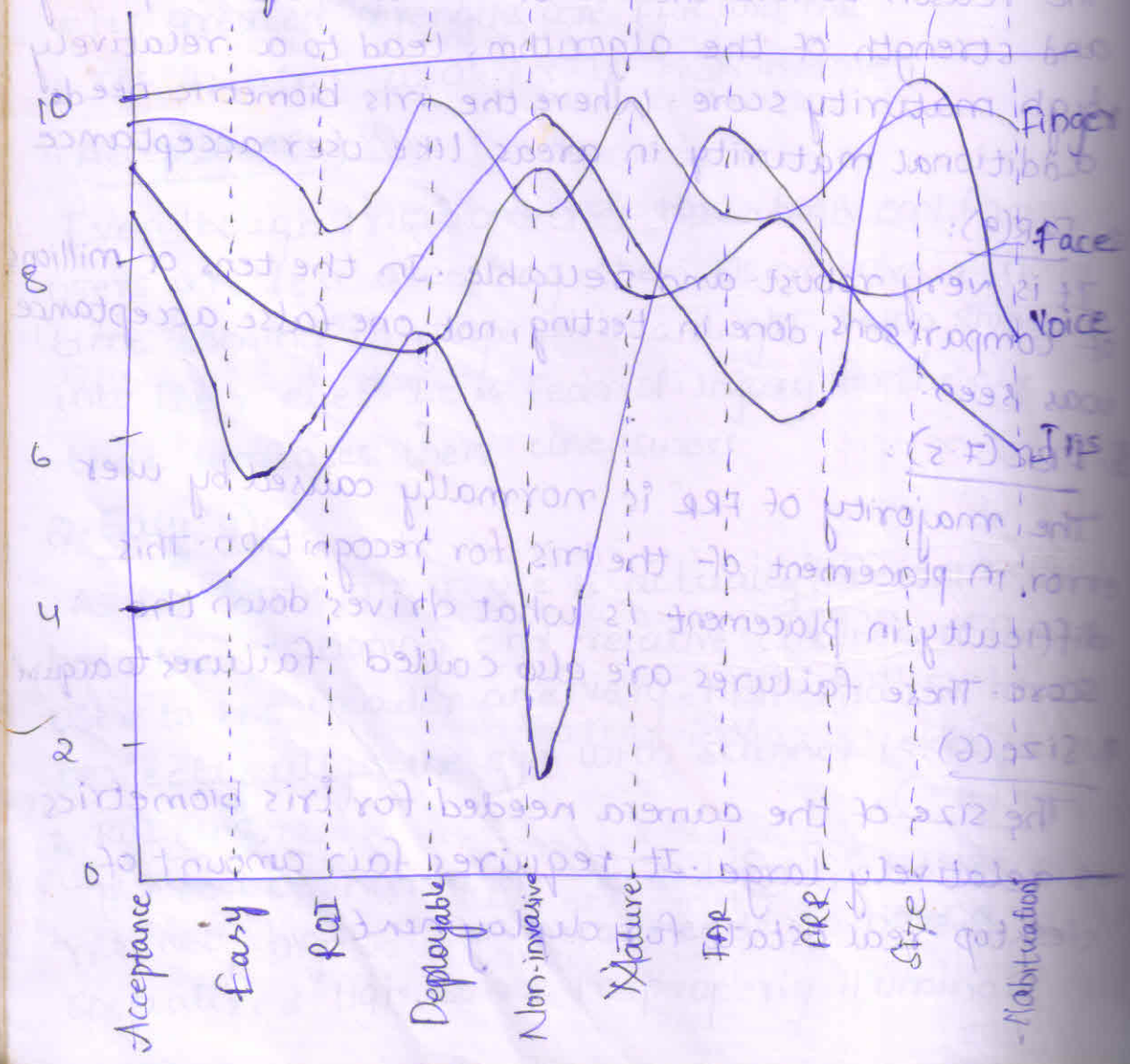
The size of the camera needed for iris biometrics is relatively large. It requires fair amount of desktop real estate for deployment

10. Habituation(5):

It requires user to be highly habituated. User need to present the iris to the camera in just right way. This is difficult because user may have a slight fear of light being shined into eye or hard time holding his/her head still

The choice of Biometric for Network Access:

* The closest overall to being ideal is fingerprint biometric,
* Fingerprint biometrics are easily deployed
* The reasons for this are their overall general suitability for use and their robustness



Finger scan

How finger s

1) Attacking

We all ha
villian fakes
done throug
removal of
detailed "fa
faked need

Mitigating

1) Most late
2) Most sur
are not th
3) The use o
"rinse-lath
4) Use a s
5) Random
6) Use mul

2) Using artif

As we saw
latent prints
exploited. T
left on the
would need
finger place

Artifact

Mitigating

1) Remove
2) Use aliv
3) Require
the same

Finger scan Spoofing:

How finger scan biometric can be spoofed?

1) Attacking the physical finger:

We all have seen this in movies, where the hero or villian fakes someone's fingerprints. This is normally done through the lifting of a latent print or the removal of the finger itself. To get a sufficiently detailed "fake finger". The user having his/her finger faked needed to be present.

Mitigating this attack:

1) Most latent prints are partial
2) Most surface that could be used for latent prints are not that easy to work with
3) The use of cyanoacrylate is not exactly a "rinse-lather-repeat" procedure
4) Use a sensor with "alive-and-well" detection election
5) Random finger authentication
6) Use multi-factor authentication

2) Using artifacts:

As we saw in the attack on the physical finger, the latent prints or artifacts we leave behind can be exploited. This particular attack focuses on artifacts left on the scanning device itself. The sensor would need to be fooled into thinking a new finger placement has taken place and image the artifact.

Mitigating this attack:

1) Remove the artifact
2) Use alive-and-well detection
3) Require that the biometric system not accept the same print twice in a row

3) Attacking the communicating channels:

If an attacker cannot compromise a system at the point of collection, the next logical spot to compromise is the communication path. If the information being transmitted could be changed so that a false positive or a false rejection occurs, the attackers may physically tap the line between the device and the PC. He/she could install trojan software on the PC to interrupt the template before local or remote comparison. Lastly, the attacker may try to replay a previously succesful authentication attempt

Mitigating this attack:

1) Real time line monitoring
2) Trojan software
3) Prevent replay attacks

4) Compromising the template:

Moving up the attack food chain, if the capture and communication of the comparison template prove to the impossible, then a compromise of the stored reference template might be attempted. To modify the reference template might be attempted. To modify the reference template, an attacker could attack the medium on which the template, or the template itself while in transit to the comparison has

Mitigating the attack:

1) Protect the storage medium
2) Protect the storage host
3) Protect the template in transit

5) Attacking the fallback system:

In any biometric system, there will never be 100% coverage of the user base. Additionally some users will have been failings from time to time that will require them to use a different factor for authentication. These fallback system are also open to attack. If the strongest point of a system is the ~~bio~~ biometric aspect, then an attacker will focus on the weaker part. In general, this is the fallback system

Mitigating this attack:

Because this type of attack is very fluid and changes from biometric system to system. The best policy to adopt is to make the fallback as strong as possible. If the fallback of your users is 'a userID and password, then make the password sufficiently strong to prevent password attacks.

Facial Scan:

How can facial biometric be spoofed:

Attacking the physical face:

Face biometric are passive. That is a biometric sample can be taken from you without your knowledge or consent

A two dimensional image:

This is normally a photograph or an enlargement that is present to a facial scanner. This method generally works for system that do not use active eye recognition or depth perception for face acquisition.

A two-dimensional image with eye cutouts:
This is good for scanners that require the acquisition of the face from the pupil location. The spoofer takes the victim face cuts out the pupils to show through

Replay of captured vedio:
This is generally done through the clandestine gathering of video footage showing the face of inteded victim.

Mitigating this attack:
While not every attack is fool proof, many are very close to always compromising the system. Once a counter measure is introduced, the spoofer can take it to the next level
In the above attacks, the spoofed image could either moved or imaged in such a way to make it fool the system what all the spoofing methods had in common was that the spoofed image need to be recorded.

Using Artifacts:
Since face biometrics are passive and do not require the user to actively submit to measurment, there is no physical contact between the user and the scanner. This means that the artifacts left by facial scanning are different from the left by fingerprints.

Mitigating this attack:
To mitigating this attack, do not use a physical for the video stream or if needed, encrypt it using PKI. This way only the process can read the content and the secret used for encrypting is not shared embedded in application itself

Voice scan spoofing:

How can this biometric be spoofed?

* It was accepted that even humans can be fooled into thinking we recognize a voice when we donot If this is the case, it is belivable and to be expected that a voice biometric system could be fooled as well
* While it is generally accepted that voice biometrics do not provide same level of FAR as other biometrics
* It offer very attractive attributes such as high user acceptance and low hardware cost

Attacks on a voice biometric system fall into following categories:

- Attacking the physical voice
- Using artifacts
- Attacking the communications
- Compromising the template
- Attacking the fallback system

Attacking the physical voice:

During the discussion of which algorithm to pick, it was noted that a decision had to be made between user convenience and security

After evaluating the tradeoff, if the company decision was for convenience, then the system is much more susceptible to things like replay attacks from a recorded voice. If on the other hand security won out over convenience, then the system is stronger and less likely to be compromised

Using artifacts:

The artifacts used for the voice biometrics are not of the same type as those used for other biometrics

The recorded artifacts i.e., the user's voices, are then used as the basis for an attack

Mitigating this attack:

* The best mitigation for this type of attack is to use an algorithm that has a sufficiently large lexicon. The lexicon should also use less common words along with the standard digits. This way, it is less likely in normal conversation to use one of the special words from the lexicon
* Another counter measure can be to have challenge phrases presented to the say in a limited amount of time. This way, the spoofer would need to have the lexican recorded for the particular user and be able to produce the challenge words in required amount of time.

Iris scan spoofing:

How can this biometric be spoofed?

The iris is an extremly difficult triat to spoof, yet there have been attempts at spoofing Attacks on the iris biometric fall into following categories

- Attacking the physical iris
- Using artifacts
- Attacking the communications
- Compromising the templates
- Attacking the fallback system

Attacking the physical iris:

One attempt at spoofing was made by CT of a germany. In this spoof, the company printed a high-quality digital image of an iris on to paper could present his/her pupils along with the faked iris image, CT succeded in getting the

system to capture an image and successfully authenticate. This spoof was possible due to the robustness of iris algorithm.

Mitigating this attack.

To mitigate against this particular attack, a check was added to the algorithm to look for a telltale signature created by the printing process and observed during the 2-D fourier power spectrum analysis.

Using Artifacts:

The artifacts used for iris biometrics are not of the same type as those used for other biometrics. The only recorded artifact i.e., the user's iris, must be used as the basis for an attack.

good (4) JW 11/2/19

1) Write two benefits of biometric fraud detection system?

Ans: Identification systems are deployed to determine whether a person's biometric information exists more than once in a database. By locating and identifying individuals who already registered for a program or service, biometric can reduce fraud.

2) Define failure to enroll rate?

Ans. A system failure to enroll rate represents the probability that a given user will be unable to enroll in biometric system. FTE is occured when user's have insufficiently distinctive or replicable biometric data or when the design of the biometric solution in such that providing consistent data is difficult

3) What are the features of fingerscan technology?

Ans.

4) List out strengths of facial scan Technology?

→ Ability to leverage a existing equipment and image processors

→ Ability to operate without physical contact or user complexity

→ Ability to enroll static images

5) List the components of iris scan technology?

→ Iris scan system compromise frontend acquisition hardware along with local or central processing software also requires camera technology and specialized devices that provide necessary infrared

. Illumination
In desktop cameras, with vedio camera functionality along with iris scan functionality

5) List out other physical and behavioural biometric systems

Physical → Hand scan Technology, Retina scan Technology, AFIS

Behavioural → Signature scan, Keystroke scan technology

6) What are the limitations of voice scan technology?

→ Effect of acquisition devices and ambient noise on accuracy
→ Perception of low accuracy
→ Lack of suitability for today's PC usage.
→ Large template size

8) List the 5 elements of biometric solution matrix?

Biometric solution matrix is a guide to deploying biometrics for a particular applications, designed to help deployers. Assess the nature of their specific authentication problem.

Five elements are

→ Urgency, Scope, Effectiveness, Exclusivity, Receptiveness

9) What are the best practices of IBG bio-privacy?

→ Limit system scope
→ Data protection
→ Use control of personal data
→ Disclosure, auditing and accountability

10) Define FAR?

11) List the recommended systems for network security

→ Finger scan technology
→ Facial scan technology
→ Voice scan technology
→ Iris scan technology

- Defining th

1) Criminal I

→ It is the
or verify th
in a law
→ The prima
an individu
process

2) Retail/ATM

→ It is the
the identity
transactions
→ This biomet
mechanism
photo identi

3) E-Commer

4) PC/Netwo

5) Physical Acc

6) Citizen I

7) Surveilla

Defining the seven Biometric Applications:

1) Criminal Identification:

→ It is the use of biometric technology to identify or verify the identity of a suspect or individual in a law of enforcement

→ The primary role of biometric is to identify an individual inorder to proceed with, or halt a process

2) Retail/ATM/Point of Sale:

→ It is the use of biometrics to identify or verify the identity of individuals conducting in-person transactions for goods and services.

→ This biometric is used to replace authentication mechanism such as presenting cards, entering PIN, photo identification or signing one's name

3) E-Commerce/Telephony.

4) PC/Network Access.

5) physical Access/Time and Attendance.

6) Citizen Identification.

7) Surveillance.