

Voice Biometrics Introduction

Presented by: Opus Research
www.opusresearch.net
P | 415-904-7666
E | info@opusresearch.net

Voice Biometrics and Speaker Verification

- Voice Biometrics is a ***technology***
 - Captures an utterance from a live caller
 - Compares it to previously stored “voiceprint”
 - Produces a score
- Speaker Verification is an ***application***
 - Employs a biometric engine plus business logic
 - Enrolls customers by obtaining voice prints
 - Compares live utterances to voice prints to produce a “pass” or “fail” responses

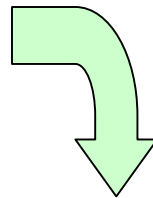
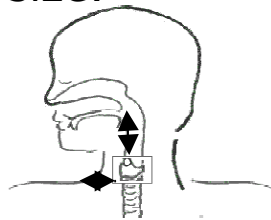
Components of Robust Speaker Verification

- The Core Verification Engine
 - Takes a voice sample (“utterance”) and compares it to a voiceprint (“template”)
 - Confirms who said it
- The Core Recognition Engine
 - Compares utterance to ASR grammar
 - Determines what was said
- The Business Logic
 - Decides if the caller passes or fails; if re-prompts are required; if other factors need to be involved

What is a Voice Print?

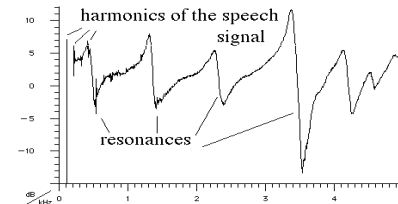
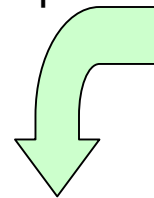
Physical Characteristics

The unique physical traits of the individual's vocal tract, such as shape and size.



Behavioral Characteristics

The harmonic and resonant frequencies, such as accents, the speed of your speech, and how words are pronounced and emphasized.



Voiceprint - Together these physiological and behavioral factors combine to produce unique voice patterns for every individual

Speaker Verification vs. Speaker Identification

- For ***Verification:***
 - User claims an ID
 - Application matches voiceprint to that claim
- For ***Identification:***
 - No claim of identity
 - ID System seeks to detect “closest match” of captured utterances to voiceprint among a population of registered users

Text Dependent vs. Text Independent

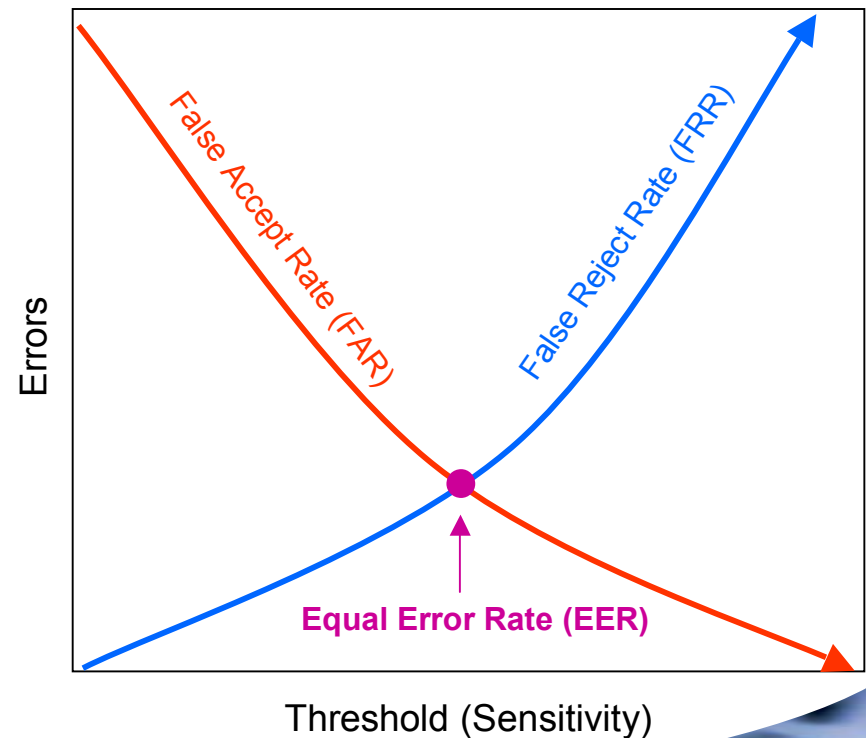
- Applications that require specific pass phrase are ***Text Dependent***
 - ❑ Require training
 - ❑ Can involve lengthy enrollment
 - ❑ Can confuse callers
- ***Text Independent*** applications can use any utterance
 - ❑ Simplify enrollment
 - ❑ Support “conversational authentication”

Evaluating Biometric Effectiveness

Two Critical Criterion:

- Equal Error Rate (EER): where False Accepts equal False Rejects
 - False Accept: Grants access to imposters
 - False Reject: Denies access to legitimate users

- Failure to Enroll (FTE): percentage of people who cannot register themselves on the system



By Any Other Name

- Tokenless Authentication
- ID Proofing
- PIN Replacement
- Voice Signature

Benefits of Voice Biometrics

- Well suited for remote authentication
 - No specialized client hardware required
 - Works from any phone
 - Supports mobility
- Cost effective to implement
 - Leverages Web and IVR investments
 - Integrates with existing authentication infrastructure
- User friendly
 - Natural feeling
 - Does not require behavioral changes

Where Voice Biometrics “Fit”

- Part of the “Front Door”
 - How may I help you?
 - Tell me your pass phrase
- PWR (Password Reset)
 - Tens of thousands served
 - Proven ROI
 - Strong proof of concept
- Point solutions

Case for Voice Authentication

- Eliminates weak security practices
- Embodies an additional factor (something you are)
- Can't be lost or stolen
- Does not require private information
- Can be combined with other technologies for multi-factor authentication
- Can be strengthened with use of random phrasing to counter impersonation and voice recording