

19 November - 1:45 p.m. – 2:45 p.m.

## Addressing the User Experience

*Speaker:*

- **David Attwater**, Senior Scientist, EIG

# Verified Usable: Addressing the User Experience

---

David Attwater  
Senior Scientist  
November 2008

# Enterprise Integration Group

---

An international professional services corporation

Established in 1993

Vendor neutral

Specializes in telephone user interface design

Design, human factors, and engineering specialists

Offices in US, Switzerland, UK, Australia.



# A Knowledge-Based Company

---

## Publications

*Bruce Balentine*

It's better to be a good machine than a bad person

How to build a Speech Recognition Application

Good listener cookbook



## Training

Improving Speech and IVR (1-Day, 2-Day, 5-Day)

Voice Biometrics and Multi-Factor Authentication (1-Day)

## Research Projects

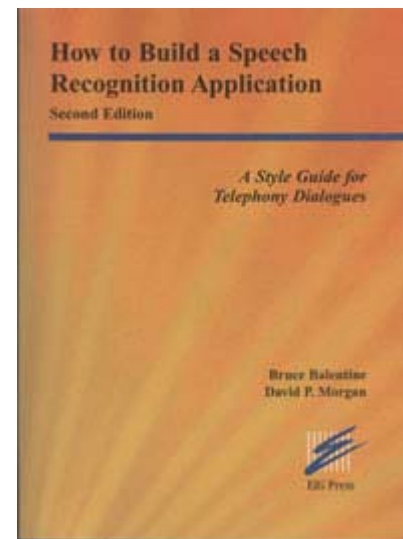
Natural Language Stabilization

Cross-Lingual Dialog Design

Turn-Taking

Mixing Speech and Touch-Tone

Multi-Factor Authentication and Voice Biometrics



# Technology and Business Drivers

---

# Technology Basics

---

## Speaker Verification Technology

Related to but not the same as Automatic Speech Recognition (ASR)

ASR recognizes what you say; SVT assesses who you claim to be

## SVT is a biometric technology

Similar to fingerprints, retinal scan, DNA

A biometric is a measurement of your biological makeup

The shape and size of your physical body determines the sound quality of your voice

Your habits are also carried in speech: dialect, accent, pronunciation, rate of speech

## SVT is growing in importance

Weak multi-factor authentication in IVR and Call Centers

Identity theft, phishing, etc. is spreading to the telephone channel

Standards groups and government bodies are regulating more strictly

- Security standards for financial services

- Privacy standards for government and healthcare

Many users don't want to use Social Security Number (SSN) or similar ID

Common personal data (phone number, date of birth or anniversary) are easy to find

Tighter multi-factor security threatens containment targets in IVRs

# Technology Overview

---

## Text Independent

- Voice print is independent of what the caller says

- Enrollment phrases need not match the phrase used for verification

- Needs more enrollment data

## Text Dependent

- Voice print is gathered for specific words or phrases

- Enrollment phrases need to match phrases used for verification

- Use voice print to verify or reject caller

## A statistical process and an uncertain medium

- Goal is to balance false positives and false negatives

# Some ID&V Terminology

---

Multi-factor authentication, factors are:

Something you know—password, PIN

Something you possess—key, swipe card

Something you are—fingerprint, iris patterns

Challenge questions plus biometric make SVT multi-factor—to imposter:

You must know data about the target user (account number, etc.)

You must also have a voice that sounds like the target user

Equal Error Rate (EER)

False Acceptance Rate (FAR)—imposters that are accepted

False Rejection Rate (FRR)—legitimate users that are rejected

Current technologies range 0.5% – 4.0% EER depending on the database test

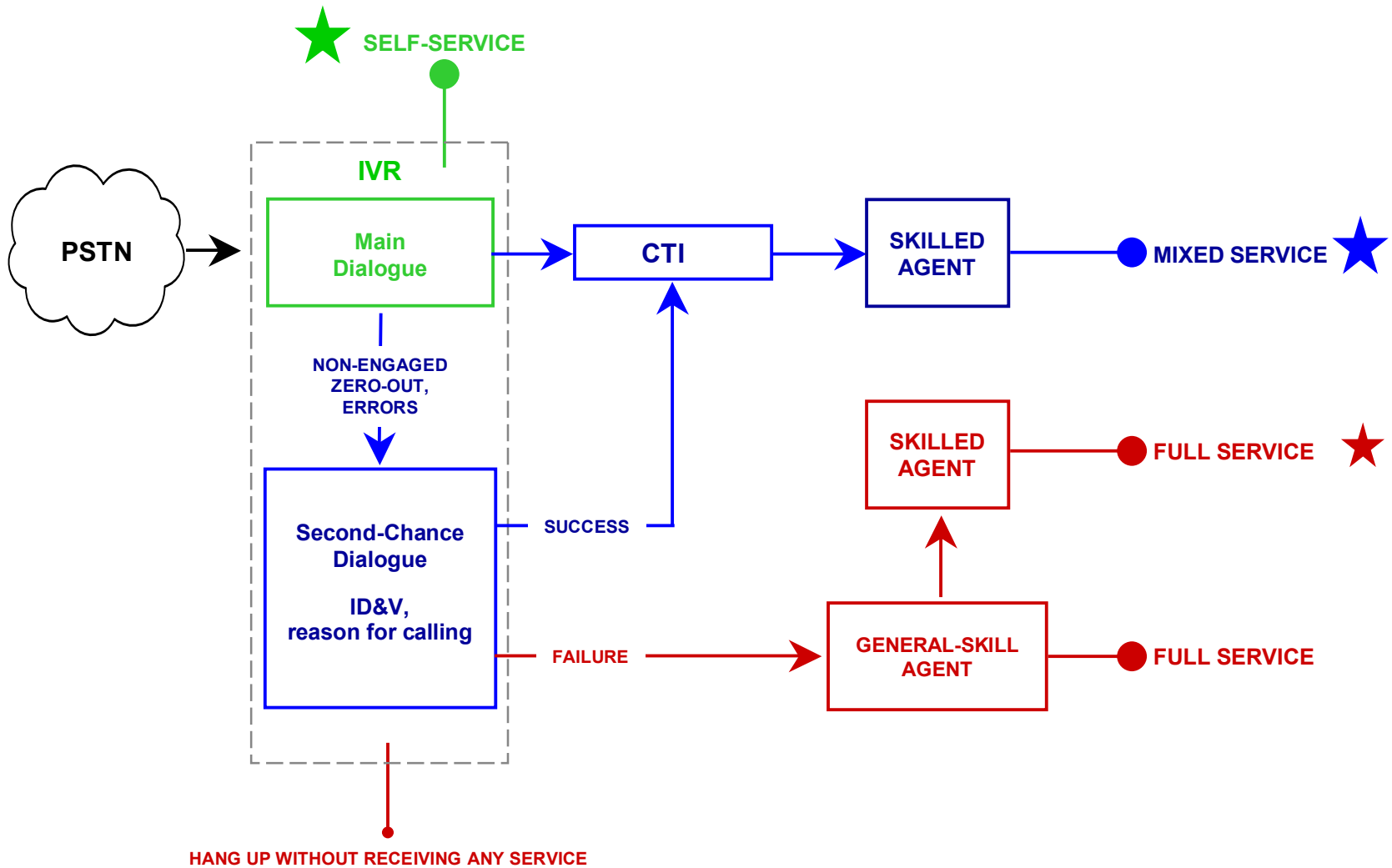
This is comparable to other biometrics (e.g., fingerprints)

Accuracy varies with data, enrollment time, number of questions, etc.

Due to multi-factor approach error rates do not define overall security levels

Typically SVT increases security levels even with a finite 'error rate'.

# Today's Call Center



# The User Experience

---

# User Experience Issues

---

How do users perceive the technology?

Customer trust and brand

Motivating and managing enrollment

Privacy versus security

Single-factor solutions

Multi-factor solutions

Managing false and correct rejection

What about temporary and permanent voice problems?

# How do users perceive the technology?

Customer intuitions about the technology are based on previous experiences

- Conditional trust in the technology when expectations are managed
- Awareness of Mimicry
- Recording attacks are rarely mentioned spontaneously
- There is valid concern over voice health and quality though (See later)

Expectations can be managed in the IVR

- Best practice dialog design can manage expectation:
- Customers are willing to seek and receive explanations from the IVR
- Clear, brief re-assurance of the technology capability during enrollment
- Be careful to explain and give help at each step

Analogy is a powerful tool

- 'its like a finger print'
- 'no one can steal your voice'
- 'your voice is unique'



*"More secure than current methods"*



*"What if someone sounds like you"*



*"It's like voice dialing..."*

# Customers trust and brand

---

## Customer trust is strongly influenced by brand perception and prior experience

Prior experience with an organisation is defining factor

If the customer trusts the corporation they tend to trust the technology

In such cases even after false rejections, confidence remains high and attitudes positive

## Reputation is a double-edged sword

Perception of security breach will impact directly on brand

Inconvenience in the interests of security will be tolerated to a point

'Visible' security breaches should be avoided

Clear reliance on multi-factor security may be important for this reason alone



*"I've banked with them for twenty years..."*



*"As long as you know its going to be the bank that uses it that's fine"*

# Motivating and managing enrollment

---

## The IVR can be the front-line for engaging callers

Customers appear comfortable using the IVR to explore enrollment

Gated multi-step engagements seem to work well supporting eager adopters and careful explorers

## Then the advisors...

Front-line advisors are a powerful force in transitioning callers from existing ID&V to biometric based security

Advisor training is paramount in persuading customers

They will win or lose the battle to persuade those who are uncertain

Give ready access to advisors but only when requested

## Then collateral ...

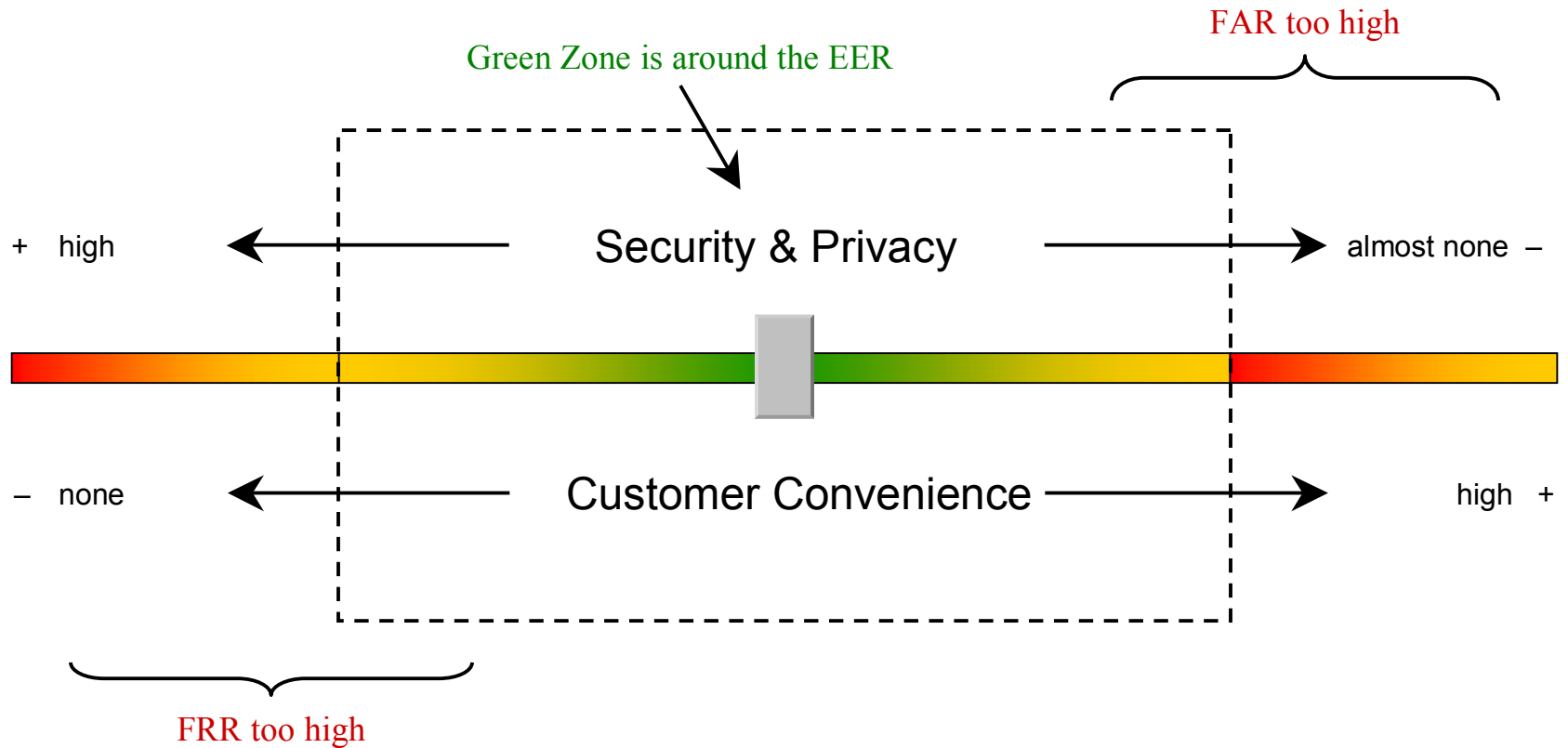
Many years of IVR experience have shown that printed collateral is rarely consulted

Consider using wider channels (such as advertising and mailing) to stimulate awareness and confidence



*"It was just right .. enough to understand the service"*

# Privacy versus security



NOTE: Regions outside the dotted lines should be avoided.

# Single factor solutions

---

Single factor biometric security is perceived as 'easy', 'straightforward', 'secure'

Replacement of PSN is perceived as a strength

'No need to remember numbers'

'Nobody can steal your voice'

The lack of a 'known' security factor is noticed but not by everyone

Most users simply accepted the PSN replacement by voice with a perception of increased security

When pressed (and shown an alternative) some callers do become concerned at a lack of a 'known' factor (see next slide)

Using a few utterances during validation is fine

Up to three questions will be accepted with no problem

It's better to just ask for more data than talk to the caller about error conditions

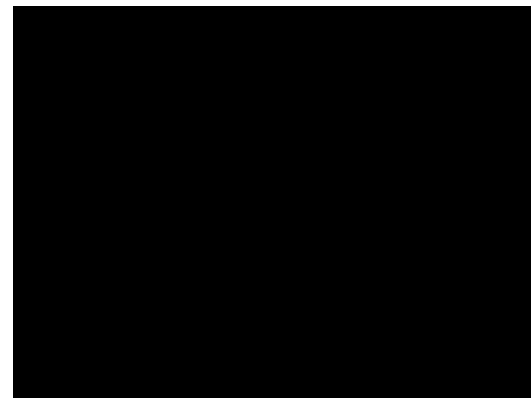
Only asking for one validation utterance is generally perceived as 'not secure enough'

The UK and USA may be different

This is probably driven by difference in IVR PIN Usage (70-85% UK versus 90% USA)



*"People Do Share PIN numbers"*



*"I often forget my password"*

# Multi-Factor Solutions

## Biometrics is preferred over other 'known data' security schemes

Recent transactions and other account data are generally not liked as a security mechanism

Personal data (mothers maiden name, memorable date) is not liked in isolation due to perceived lack of security

## Customers perceive pro's and con's for spoken personal data in conjunction with biometrics

When shown the contrast customers liked the increased security that known information brings in addition to voice biometrics

Some people mildly dislike speaking personal information out loud ('I would use it at home'). Many are comfortable however.

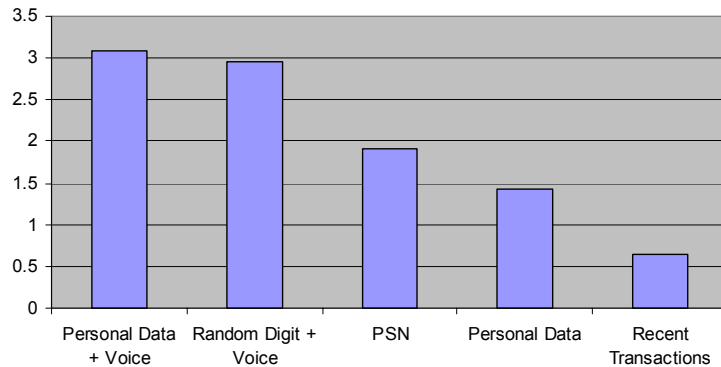
Meaningless utterances can be embarrassing (e.g. '1..9', a 4-digit random scheme is like a PSN and is acceptable)

## Additional factors are likely to be important in most secure propositions

Do not sacrifice actual security for simplicity, customers do not mind investing in security.

Consider using Touch-Tone to ask additional easily remembered pieces of known information (e.g. memorable year)

May also be central to managing false rejection



User preference ranking for types of security  
High=Preferred



*'I would add in a couple more just to be sure'*

# Managing False and Correct Rejection

---

## Customers will only tolerate infrequent false-rejection

In-frequent rejection will be tolerated and may even increase perception of security

Its much better to keep asking questions than to declare error conditions

Customers actually perceive increased levels of security as you ask them for more information

It is the inability to respond to security questions that frustrates customers – not the presence or even the quantity of them

## Customers like agent back-up on failure but only if they can do something to help!

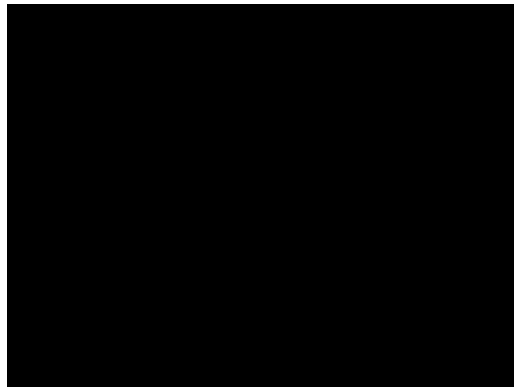
Establishing policies on false rejection are the single most difficult challenge to proposition development

In usability test conditions customers respond well to the message 'you cannot proceed without passing voice verification'

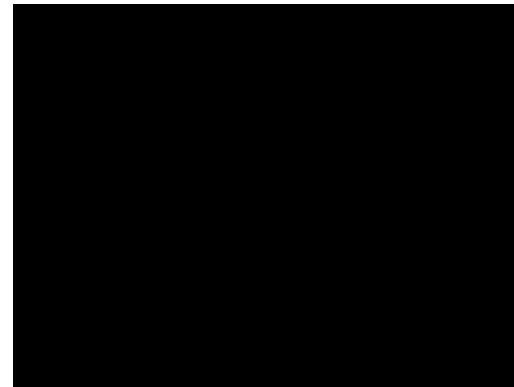
Perceived increase in security because fraudsters will have to face a personal challenge

Customers strongly disliked speaking to an agent only to be told that they must return to the IVR for re-validation

One point where some risk can be managed is offering post-enrollment tests to let customers try out their new voice prints securely



*“ .. a bit frustrated. It wouldn't recognise my voice.”*



*“If it's just a one off or every so often its no problem”*

# What about temporary and permanent voice problems?

---

Instinctive understanding that variation in voice quality will be a challenge

Temporary problems - Colds, Sore Throats, Drift of voice over time

Permanent problems – Damaged voices, Chronic conditions

Policies need to be in place and understood

From a security point of view this is analogous to the forgotten PIN problem

However emotional context is very different.

Customers are more forgiving when they understand the causes of failure

Disability awareness and rights

The selective ability to opt-out is almost certainly going to be a requirement



*"I had laryngitis. I'd like to have the option."*



*"I have a problem with my voice"*

# Conclusions

---

Users lean on metaphor and experience to understand the technology

User trust is brand-based then experiential – it is not based on technology

IVRs have an important role to play managing expectations and trust

Choose your place on the privacy/trust spectrum

Don't be afraid to use repetition for single factor solutions

Multi-factor solutions can be subtle blends designed to manage actual and perceived risk

Avoid displaying technology error and think about lock-out policies very carefully

Disability rights and temporary disablement will require robust policies

# Contact Information

---

Enterprise Integration Group, Ltd  
13 Windsor Road  
Southport, UK PR90SG  
+44 1704 53 22 27

EIG International AG  
Stampfenbachstrasse 119  
PO Box 681  
8035 Zurich, Switzerland  
+41 44 360 50 13

<http://www.eiginc.com>

Enterprise Integration Group, Inc.  
2817 Crow Canyon Road, Suite 100  
San Ramon, California 94583 USA  
+1 925 735 1700 or +1 888-EIG-4IVR

EIG/UCMS  
Level 6, 15 William Street  
Melbourne, Victoria 3000  
Australia  
+61 0447 336 364

[david@eiginc.com](mailto:david@eiginc.com)  
[rex@eiginc.com](mailto:rex@eiginc.com)