

May 4 - 1:45 p.m. – 2:45 p.m.

Voice Biometrics in the Contact Center

Speaker:

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

Voice Biometrics in the Customer Contact Center

David Attwater
Senior Scientist

May 2010

About Enterprise Integration Group

An international professional services corporation

Established in 1993

Vendor neutral

Specializes in telephone user interface design

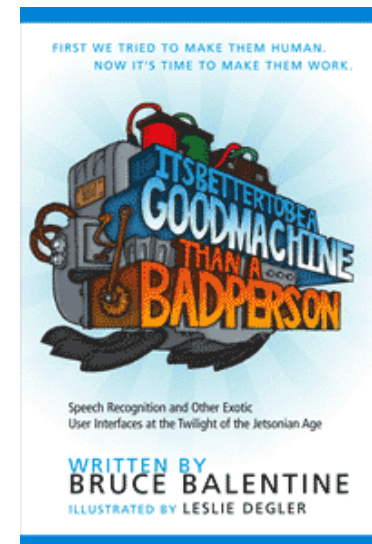
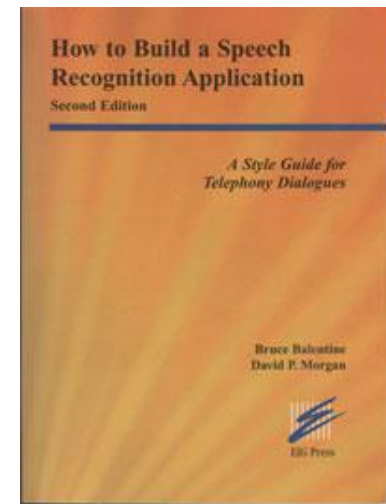
Design, human factors, and engineering specialists

Offices in US, Switzerland, UK, Australia

Publications

How to build a speech recognition application

Its better to be a good machine than a bad person



Technology Basics

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, voice

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)

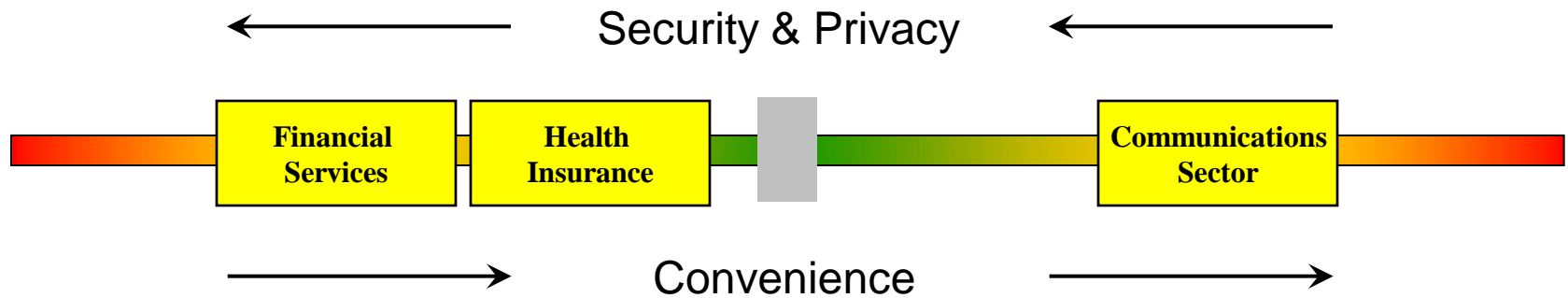
Accuracy varies with data, enrollment time, number of questions, etc.

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

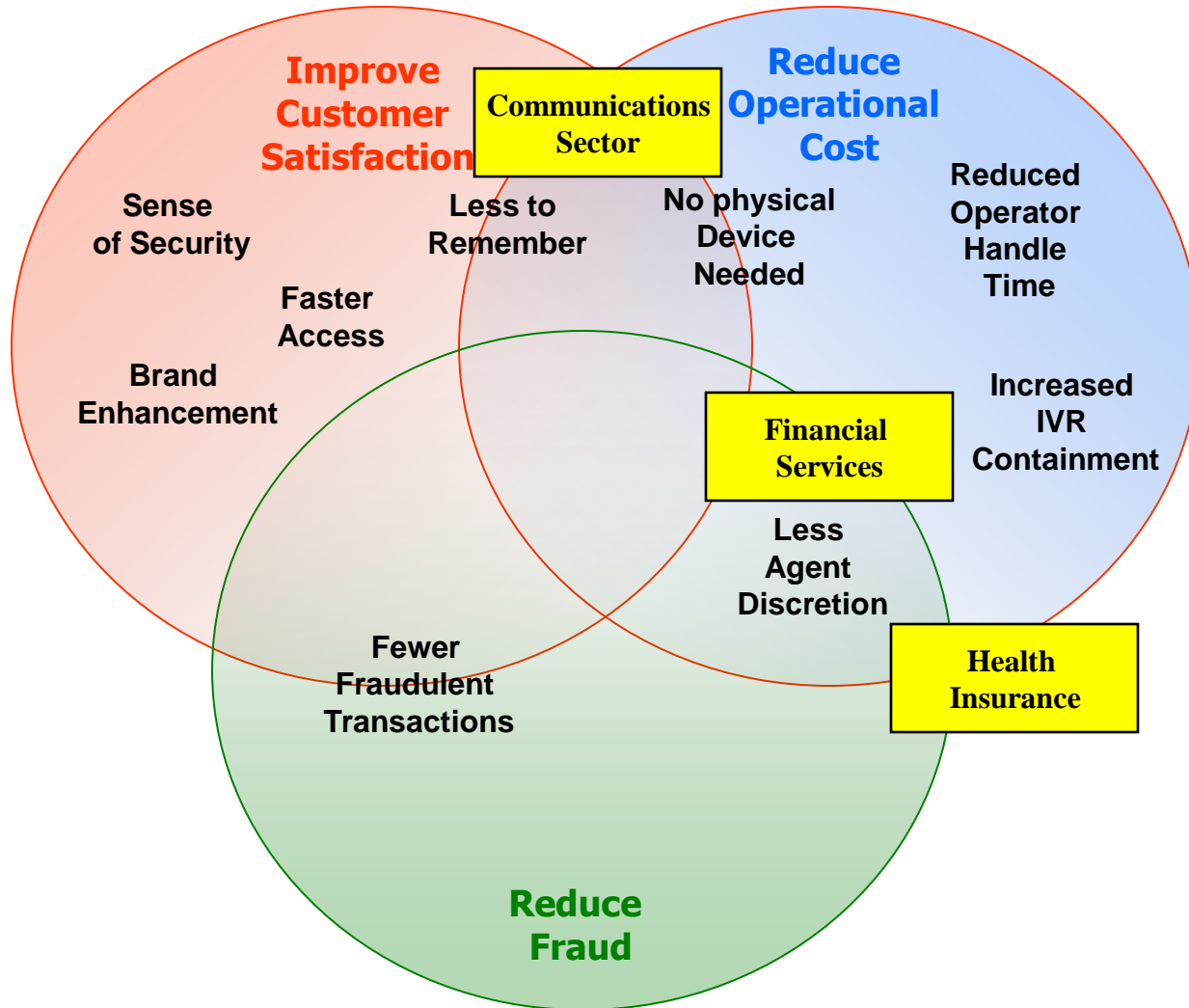
Typically SVT increases security levels even with a finite 'error rate'.

Business Drivers and Risk

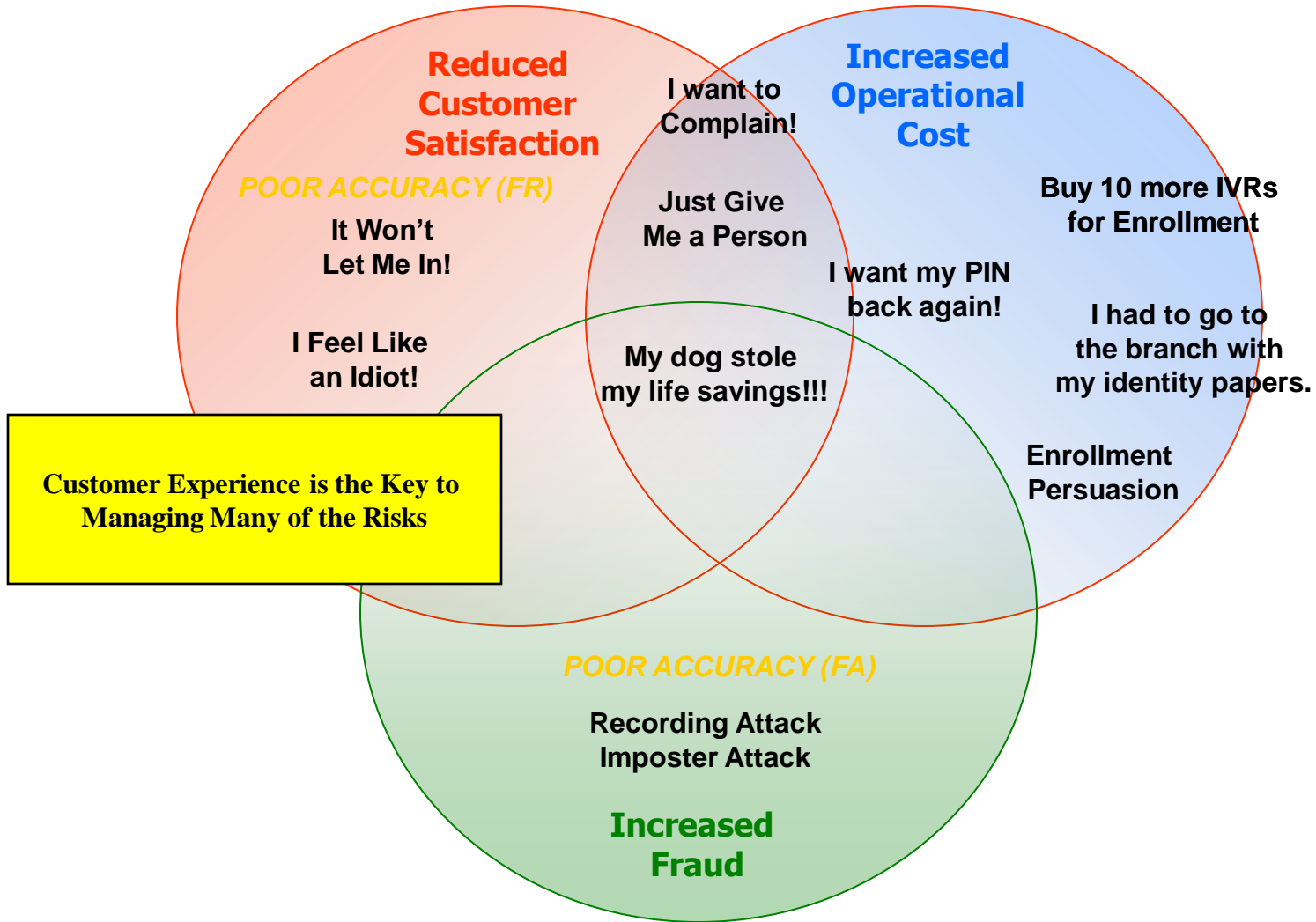
Security versus Convenience



The Business Case



The Risk



Customer Experience

User Experience Questions

How do users perceive the technology?

Why do customers choose to sign up?

How do you manage successful enrollment?

Is PIN replacement good enough for customers?

What happens when things go wrong?

Should we ask for additional private data and how?

Should we ever rely on voice alone?

How do customers perceive the technology?

Perception of technology is based on prior experiences and intuition

Prior experiences of speech recognition

Intuitions about human language

Cultural programming



“It’s like voice dialing....”



“What if someone sounds like you”

Why do customers choose to sign-up?

Customer concern over fraud is relatively low

Typically less than 25% are 'very concerned' about fraud or identity theft

Convenience appears to be a stronger motivator than fraud

When asked upwards of 85% say convenience is the primary motivator

Even those who are concerned about fraud give the same answer

Privacy and trust are brand dependent



"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"

How do you manage successful enrollment?

People will invest time in things they care about

The IVR can effectively manage the process

- Analogy is important (“It’s like a fingerprint”)

- Choice of fast or slow lanes

- Ability to break out essential

Using is believing

- Test run after enrollment

- Back-out

Advisors are essential back-up

- Training is essential

- They need to believe in it

Then collateral ...

- Rarely a deciding factor.

- Consider TV and exemplars



“It was just right .. enough to understand the service”

Is PIN replacement good enough for customers?

Many people are happy with PIN security

PIN Penetration is high. (70-85% UK, 90% USA)

Many people consider PIN usage secure and convenient

But those who have difficulty recalling PINs like the convenience

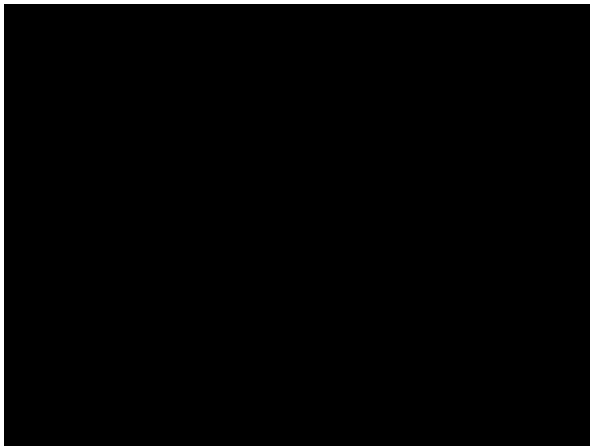
'No need to remember numbers'

'Nobody can steal your voice'

Convenience dominates over security

The lack of a 'known' security factor is noticed but does not seem to dominate

But it has to actually work....



"I often forget my password"



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

What happens when things go wrong?

The single most common cause of cancellation is accuracy

Majority of people who cancel do within less than 5 uses

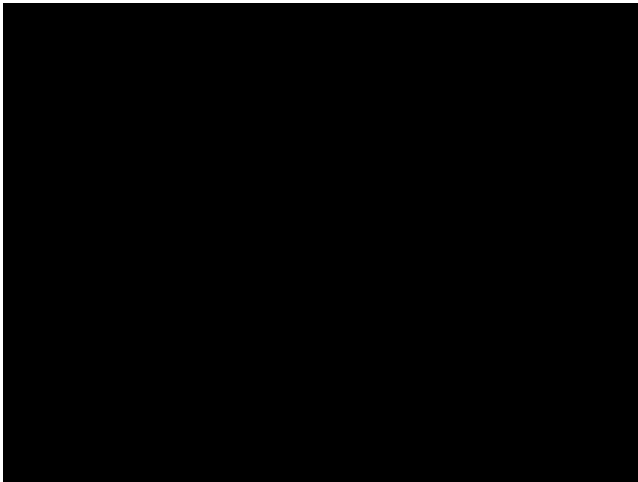
False rejection is deeply inconvenient and features way ahead of other things such as call duration, speaking out loud and security concerns.

A longer journey is preferable to an insurmountable obstacle

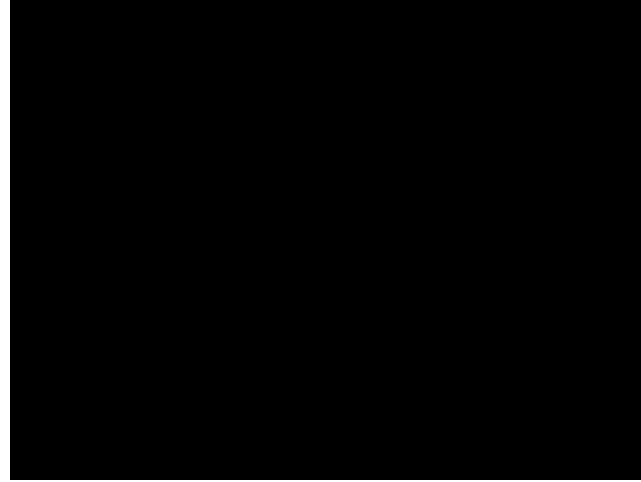
Up to three questions will be accepted with no problem

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'



".. a bit frustrated. It wouldn't recognise my voice."



"If it's just a one off or every so often it's no problem"

So should we ask for additional private data and how?

Biometrics is preferred over other 'known data' security schemes

Recent transactions and other account data are generally not liked

Personal data (mothers maiden name, memorable date) is perceived as insecure

Pro's and con's for spoken personal data

Customers like being asked more information but only if they know it.

Some dislike speaking personal information out loud ('I would use it at home').

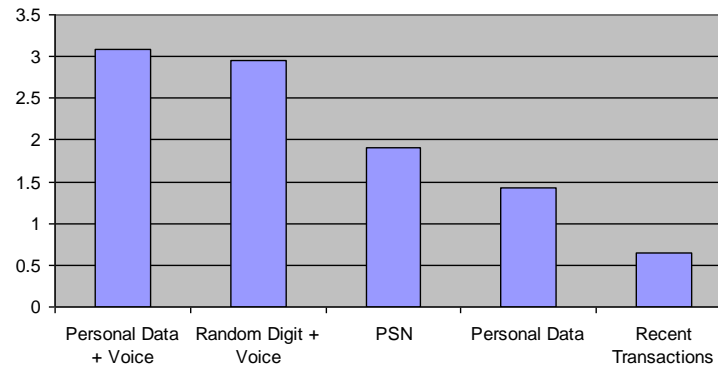
Meaningless utterances can be embarrassing (e.g. '1..9', a 4-digit random scheme is like a PSN and is acceptable)

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 Touch-Tone to ask additional easily remembered information (e.g. memorable year)

May also be central to managing false rejection



User preference ranking for types of security
High=Preferred

Should we ever rely on voice alone?

Customers are clear that they would like the option to opt in our out

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

Permanent problems – Damaged voices, Chronic conditions

Policies need to be in place and carefully worked through

A visit to a branch with identity papers costs everyone involved dearly

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

Conclusions

Convenience is valued more highly than security by customers

Users lean on metaphor, brand and experience to understand the technology

IVRs have an important role to play managing the enrollment process

Reliance on technology is dangerous and accuracy really matters


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

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

Create a subtle Multi-factor blend designed to manage actual and perceived risk

Disability rights and temporary disablement will require robust policies

Contact Information



ENTERPRISE
INTEGRATION
GROUP

DAVID ATTWATER
Senior Scientist

13 Windsor Road
Southport PR9 0SG
United Kingdom
Office: +44 1704 532227
Mobile: +44 1704 530149
Fax: +44 792 1244 038
david@eiginc.com

Contact Information

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

EIG International AG
Stampfenbachstrasse 119
PO Box 273
8042 Zurich, Switzerland
+41 44 360 50 13

<http://www.eiginc.com>

Enterprise Integration Group, Inc.
3767 Crow Canyon Road
San Ramon, California 94582 USA
+1 925 735 1700 or +1 888-EIG-4IVR

david@eiginc.com
rex@eiginc.com