Securing Conversational Interfaces

FEBRUARY 2020

1441 BROADWAY AVE
NEW YORK, NEW YORK 10018
www.idrnd.ai
Conversational Interface
Security Today

No Security

- Simple, low-risk inquiries
- General help, FAQs
- Smart Speaker commands

Authenticated Session

- Personal, account-specific and sensitive information
- Often requires OTPs, passwords, knowledge-based authentication or transfer to a different channel

**Adds friction to the UX and not strongly secure**
What is the IDEAL Customer Experience for Authenticating in a Conversational Interface?
Friend-like Authentication

- How you look  
  Facial Biometrics

- How you talk  
  Voice Biometrics

- Your behavior  
  Keystroke Dynamics
SafeChat™ Biometrics Demo: Frictionless User Experience In Action

BIOMETRIC VIRTUAL ASSISTANT

ASK A QUESTION (TYPE OR SPEAK)

REAL TIME FRICITIONLESS BIOMETRIC ID

SafeChat DEMO
Liveness Is Critical!

Does the sound emanate from a human vocal tract or a replay device?
## Synthesized Voice Samples

All detected as spoofs

<table>
<thead>
<tr>
<th>Synthesizer</th>
<th>Sample</th>
</tr>
</thead>
<tbody>
<tr>
<td>Lyrebird</td>
<td><img src="image" alt="Speaker" /></td>
</tr>
<tr>
<td>Google Tacotron</td>
<td><img src="image" alt="Speaker" /></td>
</tr>
<tr>
<td>Google Wavenet</td>
<td><img src="image" alt="Speaker" /></td>
</tr>
</tbody>
</table>
#1 Voice Biometric Liveness Anti-Spoofing

ASVspoof 2020: Automatic Speaker Verification Spoofing and Countermeasures Challenge for Logical Access (LA)

ID R&D is a clear leader in the largest voice biometric anti-spoofing challenge to date

The Challenge was designed to test an ability to distinguish between human voice and a synthesized human voice

Figure 2: Bona fide/spoof detection error trade-off (DET) profiles for the baseline system (B02) and each of the 48 primary submissions to the LA ASVspoof 2019 challenge.
Liveness Is Critical!

Is the face a live human face or a photograph, video, or mask

Facial Liveness detects printed photos, cut outs, videos and masks
Benefits

Best possible **User Experience:**
No passwords. No PINs. No friction!

**Stronger Security**
1. Minimizes social engineering and hacking threats
2. Continuous authentication
3. Invisible to a fraudster

Easily integrated to any conversational interface
Hungry? Just say “Get Pizza” to order now and save!
Summary

✓ Biometrics enables frictionless authentication for conversational interfaces

✓ The impact is the best possible user experience with far stronger security than current MFA methods

✓ Implementation is possible TODAY
Thank You
# ID R&D Capabilities

## ID R&D Solutions

<table>
<thead>
<tr>
<th>Feature</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Text Dependent Voice Biometrics</td>
<td>Verifying identity through a spoken passphrase</td>
</tr>
<tr>
<td>Text Independent Voice Biometrics</td>
<td>Verifying identity from conversational speech</td>
</tr>
<tr>
<td>Voice Anti-Spoofing</td>
<td>Detecting whether a live person is speaking</td>
</tr>
<tr>
<td>Sound Event Recognition</td>
<td>Baby crying, dog barking, gun shots, glass breaking, etc.</td>
</tr>
<tr>
<td>Facial Liveness</td>
<td>Detecting whether a selfie is a live person or a photograph</td>
</tr>
</tbody>
</table>
Two Tests To Detect Cloning

2. Does the sound contain artifacts of synthetic speech?

Synthetic speech and converted speech contain artifacts that often are not distinguishable by the human ear.
ID R&D Antispoofing Engine

Anti-Spoofing analyzes acoustic features with Deep Neural Networks
Spoofing Data Collection

- **Late 2018**
  - Collected by ID R&D: 58%
  - All publicly available: 42%

- **Mid 2019**
  - Collected by ID R&D: 88%
  - All publicly available: 12%