NUANCE | WHAT'S NEXT BLOG

Autenticación y Prevención del Fraude, Interacción con el cliente multicanal

Deepfakes vs seguridad biométrica (y por qué la biometría de voz siempre gana)

Brett Beranek | Vice President & General Manager, Security & Biometrics

5 septiembre 2022

¿Es la voz de tus clientes? ¿O es una simulación informática? A medida que los deepfakes parecen más auténticos, es normal preguntarse sobre la capacidad que tienen de engañar a las distintas medidas de seguridad biométricas. Sin embargo, entender la evolución de la biometría de voz, una tecnología que nació para luchar contra el crimen, debería tranquilizarnos.

Los deepfakes en vídeo aparecen con cada vez más frecuencia en los titulares. El año pasado fueron las imitaciones de Tom Cruise, y este año las imitaciones del presidente ucraniano, Volodymyr Zelenskiy. Este tipo de historias normalmente suscitan preocupación en las compañías que se esfuerzan por prevenir el fraude y proteger a sus clientes con seguridad biométrica.

Al fin y al cabo, si un estafador es capaz de recrear la voz y la imagen de un cliente, ¿puede ser capaz de hacer lo mismo para entrar en las cuentas protegidas con tecnología biométrica de ese cliente? La respuesta es no, no es tan simple, especialmente cuando hablamos de la biometría de voz.

Para entender el por qué, necesitas entender qué diferencia a la voz de otras modalidades biométricas y cómo ha evolucionado la tecnología en los últimos diez años.

¿Por qué identificar a alguien por su voz es comparativamente más complicado?

Antes de unirme a Nuance para dirigir el negocio de biometría de voz, tenía experiencia trabajando con el reconocimiento facial, el reconocimiento de huellas dactilares y en el análisis de videovigilancia. Sin embargo, la tecnología de biometría de voz me fascinó por el gran reto que representaba.

Muchas tecnologías biométricas se basan en características que son estáticas por naturaleza; la huella dactilar y las dimensiones de nuestras caras no cambian entre el momento en el que nos despertamos y en el que nos vamos a dormir. Todos sabemos que la manera en la que nuestra voz suena a primera hora de la mañana es algo distinta a como suena cuando estamos hablando con un amigo a la hora de la comida. Incluso a veces podemos modificarla intencionadamente, poniendo una voz más aguda para entretener a los niños, por ejemplo.

En este sentido, como las voces son muy variables, es necesario analizar muchos más puntos de datos para identificar al humano al que pertenece. El poder de llevar a cabo este análisis, rápidamente y a gran escala, no existía en los comienzos de la tecnología.

De la escena del crimen, al contact center

Los orígenes de la biometría de voz se remontan al campo de la ciencia forense. Por aquel entonces, los datos de voz que se analizaban procedían de conversaciones telefónicas intervenidas entre delincuentes. Con una conversación larga, y el tiempo suficiente para llevar a cabo el análisis, las fuerzas de seguridad y organismos policiales podían utilizar estas primeras herramientas de biometría de voz para identificar a un individuo y construir un caso.

Pero para que la biometría de voz funcione en un contact center o en una IVR, siendo utilizada como un factor de autenticación del cliente seguro y sin interrupciones, es necesario ser capaz de analizar muchos puntos de datos en un corto periodo de tiempo. Esto es posible con la llegada de las redes neuronales profundas.

Con las redes neuronales profundas, ya no es necesario dedicar horas para analizar muchos minutos de audio para identificar con seguridad a la persona que está hablando. Se puede identificar en tan solo medio segundo de habla natural, y con esto quiero decir que ni siquiera es necesario que digan una frase fija, pueden simplemente estar explicando sus necesidades a un agente del contact center o asistente virtual.

Otro gran avance reciente de la tecnología ha sido la producción de software en torno a estos algoritmos tan complejos, lo que ha puesto la autentificación biométrica de voz al alcance incluso de organizaciones relativamente pequeñas, como bancos regionales, bancos domésticos y cooperativas de crédito.

¿Cómo la tecnología de biometría de voz lucha contra los deepfakes?

Es evidente que los delincuentes no se han quedado de brazos cruzados en la última década. Han estado buscando formas de engañar a la biometría de voz, y eludir los procesos de autentificación que hacen uso de ella. Pero para evitar estas situaciones, nosotros también hemos trabajado en buscar esos vectores de ataque.

Desde el principio, los que trabajamos en el ámbito de la biometría de voz, sabíamos que los delincuentes intentarían engañar a la tecnología reproduciendo grabaciones de voz de otras personas diferentes. Por ello, nos aseguramos de que las soluciones biométricas de voz pudieran ser capaces de distinguir entre una voz humana real y una procedente de un audio.

A lo largo de los años, a medida que la tecnología para sintetizar o “falsificar” voces se ha hecho cada vez más fuerte y accesible, hemos trabajado para ir a un paso por delante de los delincuentes, utilizando las mismas redes neuronales profundas que han desvelado el verdadero potencial de la biometría de voz.

Cuando alguien usa un ordenador para crear una voz sintética, siempre hay pequeñas señales reveladoras. Con las redes neuronales profundas, podemos detectar estas pequeñas diferencias entre una voz natural y una sintética, y denegar a los delincuentes el acceso que desean conseguir.

Es importante también mantener la amenaza que suponen los deepfakes en perspectiva. Los criminales no suelen utilizar tecnología deepfake porque requiere de muchos recursos. La mayor parte del fraude en los canales de voz sigue basándose en tácticas más comunes, como la suplantación de identidad, las identidades sintéticas y el abuso de políticas, que la tecnología de biometría de voz también puede ayudar

a prevenir.

Mientras sigamos siendo capaces de anticiparnos a este tipo de amenazas emergentes y neutralizándolas efectivamente antes de que se materialicen, los próximos diez años van a ser aún más emocionantes, ya que la seguridad biométrica permite un nuevo mundo de interacciones remotas con los clientes.

Antes de la pandemia, algunas organizaciones todavía pedían a sus clientes que acudieran a una sucursal o tienda para realizar las actividades que suponían un alto riesgo, sin embargo, esta situación pronto desaparecerá. Gracias a la combinación de la biometría de voz junto con otros factores de autentificación y la IA, como hace Nuance Gatekeeper, estamos en el camino de una era en la que incluso las interacciones de alto riesgo pueden realizarse a distancia, de forma sencilla y con unos niveles de confianza muy altos.

Tags: Prevención de fraude, Seguridad y biometria, Falsificaciones profundas

More Information

Saber más

Escúchame hablar sobre las deepfakes, privacidad y el futuro de la biometría

Learn more

About Brett Beranek

Brett Beranek es General Manager de la división de biometría y seguridad en Nuance Communications. Antes de unirse a Nuance, ha trabajado durante más de una década como responsable de desarrollo de negocio y marketing en distintas empresas de software y seguridad. Brett posee una amplia experiencia en el campo de las tecnologías biométricas, donde es importante destacar su papel como socio fundador de la startup Viion Systems, empresa de desarrollo de software de reconocimiento facial. Su conocimiento en materia de seguridad abarca una amplia variedad de tecnologías que incluyen, desde la biometría de huella dactilar, hasta tecnologías de análisis de videos para el entorno de la seguridad física y reconocimiento de matrículas. Brett es licenciado en comercio, con la especialidad de sistemas de información por la Universidad McGill y posee un máster en marketing por la Sloan School of Management de Massachusetts Institute of Technology.

View all posts by Brett Beranek