What's next

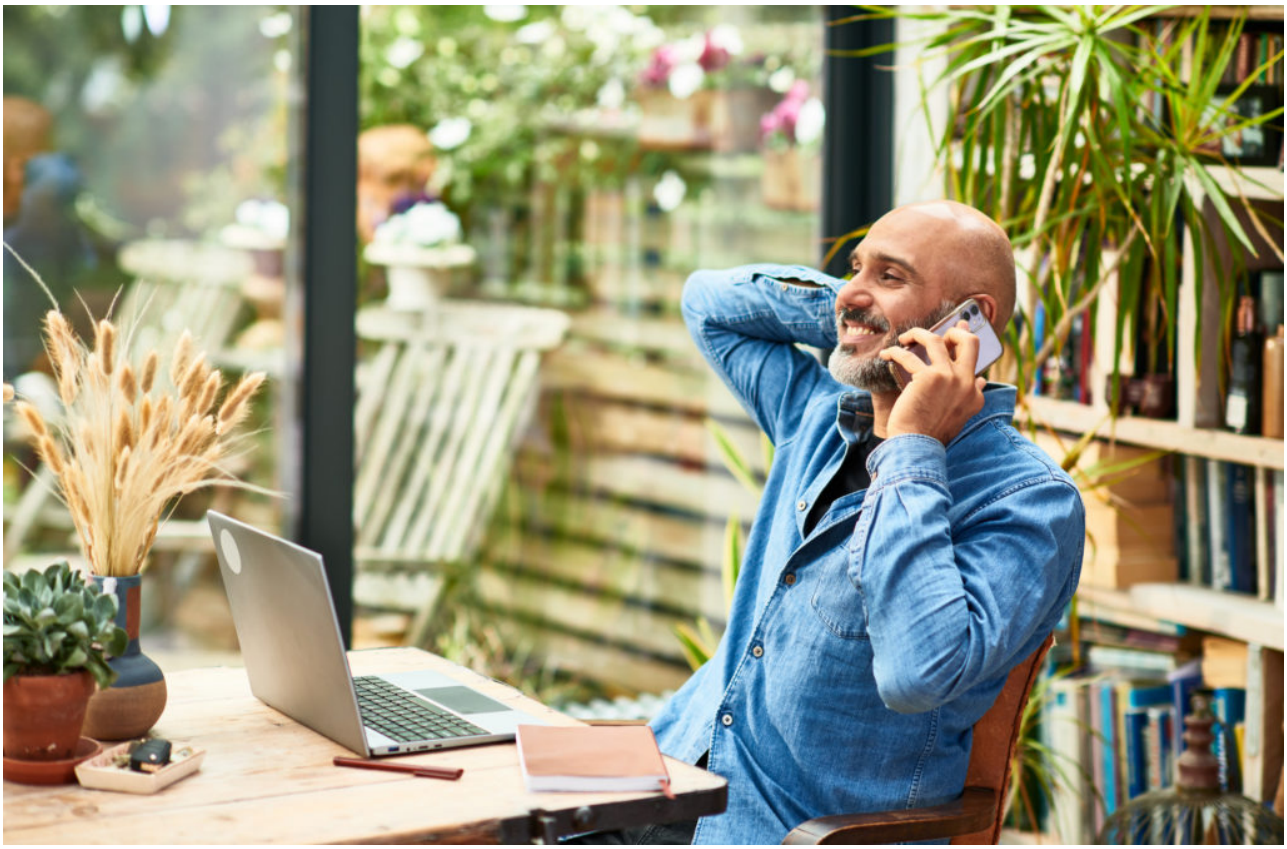
Entreprise

Deepfakes vs sécurité biométrique : pourquoi la biométrie vocale est toujours gagnante

Est-ce la voix de votre client ? Ou une simulation informatique ? Les deepfakes (ou hypertrucages) étant de plus en plus convaincants, il est naturel – et important – de se poser des questions sur leur capacité à tromper les mesures de sécurité biométriques. Mais comprendre l'évolution de la biométrie vocale, une technologie née dans la lutte contre la criminalité, devrait vous aider à avoir l'esprit un peu plus tranquille.

Brett Beranek

Posted 5 septembre 2022



es vidéos deepfakes semblent font l'actualité de plus en plus fréquemment. L'année dernière, il s'agissait d'imitations de Tom Cruise. Cette année, ce sont des imitations du président ukrainien, Volodymyr Zelenskiy. De telles histoires suscitent naturellement des inquiétudes chez les organisations qui s'efforcent de prévenir la fraude et de protéger leurs clients grâce à la sécurité biométrique.

Après tout, si un fraudeur est capable de recréer le visage et la voix d'un client, ne sera-t-il pas capable de sourire et de parler pour accéder à ses comptes sécurisés par la biométrie ? En bref, la réponse est non, ce n'est pas si simple, surtout lorsqu'il s'agit de biométrie vocale.

Pour comprendre pourquoi, il faut savoir ce qui distingue la voix des autres modalités biométriques et comment la technologie a évolué au cours des dix dernières années.

Pourquoi il est relativement difficile d'identifier une personne à partir de sa voix

Avant de rejoindre Nuance pour diriger son activité de biométrie vocale, j'avais une expérience pratique de la reconnaissance faciale, de la reconnaissance des empreintes digitales et de l'analyse de la vidéosurveillance. Mais la biométrie vocale me fascinait en raison du défi complexe qu'elle représentait.

De nombreuses technologies biométriques reposent sur des caractéristiques de nature

statique : votre empreinte digitale et les dimensions de votre visage ne changent pas entre le moment où vous vous réveillez et celui où vous vous couchez. Mais nous savons tous que le son de notre voix au petit matin est un peu différent de celui au moment où nous discutons avec un ami pendant le déjeuner. Nous pouvons même la modifier volontairement, en prenant une voix ridicule pour distraire les enfants.

Les voix étant beaucoup plus variables, il faut analyser beaucoup plus de points de données pour identifier avec certitude les personnes à qui elles appartiennent. Et la capacité d'effectuer cette analyse, rapidement et à grande échelle, n'existait tout simplement pas lorsque la technologie a vu le jour.

De la scene de crime au centre de contact

La biométrie vocale trouve son origine dans le domaine de la médecine légale. À l'époque, les données vocales analysées provenaient de conversations téléphoniques enregistrées entre criminels. Avec une conversation suffisamment longue et suffisamment de temps pour effectuer l'analyse, les forces de l'ordre pouvaient exploiter ces premiers outils de biométrie vocale pour identifier un individu et monter un dossier.

Mais pour mettre la biométrie vocale au service d'un centre de contact ou d'un SVI, pour l'utiliser comme facteur d'authentification du client sûr et transparent, il faut être capable d'analyser un grand nombre de points de données en un temps très court. Et cela n'est devenu possible qu'avec l'avènement des réseaux neuronaux profonds.

Grâce aux réseaux neuronaux profonds, il n'est plus nécessaire de passer des heures à analyser de nombreuses minutes d'audio pour identifier avec certitude la personne qui parle. Il est possible de l'identifier à partir d'une demi-seconde de parole naturelle, sans qu'il soit nécessaire qu'elle prononce une phrase spécifique (la personne peut simplement être en train d'expliquer ses besoins à un agent du centre de contact).

Une autre avancée récente et majeure de la technologie a été la production du logiciel autour de ces algorithmes très complexes, mettant l'authentification biométrique vocale à la portée même des organisations relativement petites, telles que les banques régionales, les banques communautaires et les coopératives de crédit.

Comment les technologies de biométrie vocale permettent de vaincre les deepfakes

Bien sûr, les criminels n'ont pas passé la dernière décennie à se croiser les bras ; ils ont cherché des moyens de tromper la biométrie vocale et de contourner les processus d'authentification qui l'utilisent. Mais nous avons également cherché ces vecteurs d'attaque.

Dès le départ, ceux d'entre nous qui travaillaient dans le domaine de la biométrie vocale savaient que les criminels tenteraient de tromper la technologie en reproduisant des enregistrements de la voix d'autres personnes. Nous avons donc fait en sorte que les solutions de biométrie vocale puissent faire la différence entre une voix humaine réelle et une

voix provenant d'un fichier audio.

Au fil des années, alors que la technologie permettant de synthétiser ou d'imiter des voix est devenue plus puissante et plus accessible, nous nous sommes efforcés de garder une longueur d'avance sur les fraudeurs en utilisant les mêmes réseaux neuronaux profonds qui ont révélé le véritable potentiel de la biométrie vocale.

Lorsque quelqu'un utilise un ordinateur pour synthétiser une voix, il y a toujours de minuscules signes révélateurs. Grâce aux réseaux neuronaux profonds, nous pouvons détecter les différences infimes entre une voix naturelle et une voix synthétique, et refuser aux fraudeurs l'accès qu'ils espèrent obtenir.

Il est également important de relativiser la menace que représentent les deepfakes. Les fraudeurs utilisent rarement la technologie du deepfake car celle-ci est très gourmande en ressources. La part du lion de la fraude sur les canaux vocaux repose toujours sur des tactiques plus « courantes » telles que l'usurpation d'identité, les identités synthétiques et l'abus de politique, autant d'activités que la technologie de biométrie vocale peut également contribuer à prévenir.

Tant que nous continuerons à anticiper ces menaces émergentes et à les neutraliser efficacement avant qu'elles ne se concrétisent, les dix prochaines années seront encore plus passionnantes, car la sécurité biométrique ouvre la voie à un nouveau monde d'interactions à distance avec les clients.

Avant la pandémie, certaines organisations demandaient encore aux clients de se rendre dans une agence ou un magasin pour effectuer des activités à très haut risque. Cette époque sera bientôt révolue pour de bon. En associant la biométrie vocale à d'autres facteurs d'authentification et à l'intelligence artificielle, comme le fait Nuance Gatekeeper, nous nous dirigeons vers une ère où même les interactions à haut risque pourront être réalisées à distance, avec une simplicité nouvelle et des niveaux de confiance incroyablement élevés.

Tags: Autentification Biométrique, Nuance Gatekeeper

More Information

Pour en savoir plus
Procédez aux authentifications et prévenez la fraude à l'aide de l'intelligence artificielle et de la biométrie.
Learn more

About Brett Beranek

Brett Beranek est responsable de la sécurité et de la biométrie chez Nuance. Avant de rejoindre Nuance, il a occupé, au cours des dix dernières années, divers postes de développement commercial et de marketing dans le domaine des logiciels de sécurité B2B. Brett Beranek possède une vaste expérience des technologies biométriques, notamment en tant qu'associé fondateur de Viion Systems, une start-up spécialisée dans le développement de solutions logicielles de reconnaissance faciale pour le marché des entreprises. Brett Beranek a également une expérience approfondie d'un large éventail d'autres technologies de sécurité, y compris la biométrie des empreintes digitales, l'analyse vidéo pour l'espace de sécurité physique et la technologie de reconnaissance des plaques d'immatriculation. Il est titulaire d’un Bachelor of Commerce, Information Systems Major, de l'université McGill, ainsi qu'un certificat de marketing exécutif de la Sloan School of Management du Massachusetts Institute of Technology.

View all posts by Brett Beranek