NUANCE | WHAT'S NEXT BLOG

Authentication & fraud prevention, Customer engagement

Deepfakes vs biometric security. (And why voice biometrics still wins.)

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

23 June 2022

Is that your customers' voice? Or a computer simulation? As deepfakes become more convincing, it's natural—and important—to ask questions about their ability to fool biometric security measures. But understanding the evolution of voice biometrics, a technology that was born in the fight against crime, should help you sleep a little easier.

Deepfake videos seem to be hitting the headlines ever more frequently. Last year, it was imitations of Tom Cruise. This year, imitations of Ukrainian President, Volodymyr Zelenskiy. Such stories naturally raise concerns for organizations striving to prevent fraud and protect customers with biometric security.

After all, if a fraudster is able to recreate a customer's face and voice, won't they be able to smile and talk their way into that customers' biometrically secured accounts? The short answer is, no, it's not that simple—especially when we're talking about voice biometrics.

To understand why, you need to understand what sets voice apart from other biometrics modalities, and how the technology has evolved over the last ten years.

Why identifying someone based on their voice is

comparatively difficult

Before joining Nuance to lead its voice biometrics business, I had hands-on experience working with facial recognition, fingerprint recognition, and video surveillance analytics. But voice biometrics technology fascinated me because of the complex challenge it represented.

Many biometric technologies rely on characteristics that are static in nature; your fingerprint and the dimensions of your face don't change between the moment you wake up and the moment you go to sleep. But we all know the way our voice sounds in the early morning is a little different to how it sounds by the time we're chatting to a friend over lunch. We can even modify it on purpose, putting on a silly voice to entertain the kids.

Because voices are so much more variable, you need to analyze many more data points to confidently identify the human to whom it belongs. And the power to perform that analysis, rapidly and at scale, simply didn't exist in the technology's earliest days.

From the crime scene to the contact center

The origins of voice biometrics technology lie in the field of forensic science. Back then, the voice data being analyzed came from tapped phone conversations between criminals. With a long enough conversation, and sufficient time to perform the analysis, law enforcement agencies could leverage these early voice biometrics tools to identify an individual and build a case.

But to put voice biometrics to work in a contact center or IVR—to use it as a secure, seamless customer authentication factor—you need to be able to analyze a lot data points in a very short period of time. And that's only become possible with the advent of deep neural networks.

With deep neural networks, you don't need spend hours analyzing many minutes of audio to confidently identify the person speaking. You can identify them based on as little as half a second of natural speech. (And by that, I mean they don't even need to be saying an agreed passphrase. They can simply be explaining their needs to a contact center agent.)

Another recent, major step forward for the technology has been the productizing of the software around these very complex algorithms, bringing voice biometrics authentication within the reach of even relatively small organizations, such as regional banks, community banks, and credit unions.

How voice biometrics technologies are beating deepfakes

Of course, criminals haven't spent the last decade sitting on their hands; they've been looking for ways to trick voice biometrics, and bypass authentication processes that make use of it. But we've been looking for those attack vectors, too.

From the very start, those of us working in the voice biometrics space knew criminals would attempt to trick the technology by playing back recordings of other people's voices. So, we made sure voice biometrics solutions could tell the difference between a real, live human voice and one emanating from an audio file.

Over the years, as the technology to synthesize or "deepfake" voices has become more powerful and accessible, we're worked to stay one step ahead of fraudsters—using to the same deep neural networks that have unlocked voice biometrics' true potential.

When someone uses a computer to synthesize a voice, there are always tiny, telltale sings. With deep neural networks, we can detect the minute differences between a natural voice and a synthetic voice, and deny fraudsters the access they're hoping to achieve.

It's also important to keep the threat from deepfakes in perspective. Fraudsters rarely use deepfake technology because it's so resource intensive. The lion's share of fraud in voice channels is still based on more "run-of-the-mill" tactics such as identity theft, synthetic identities, and policy abuse, all of which voice biometrics technology can also help to prevent.

As long as we continue to anticipate such emerging threats, and effectively neutralize them before they materialize, the next ten years are going to be even more exciting—as biometrics security enables a new world of remote customer interactions.

Prior to the pandemic, some organizations still asked customers to attend a branch or store to perform very high-risk activities. Those days will soon be gone for good. Through the layering voice biometrics with other authentication factors and AI—as Nuance Gatekeeper does—we're on course for an era in which even high-risk interactions can be delivered remotely, with new simplicity and incredibly high levels of

confidence.

Tags: Fraud prevention, Nuance Gatekeeper, Biometric authentication, Deepfakes

More Information

Dive deeper

Hear me talk deepfakes, privacy and the future of biometrics on the ISF Podcast—with International Security Forum Chief Executive, Steve Durbin.

Learn more

About Brett Beranek

Brett Beranek is responsible for overseeing the security and biometric line of business at Nuance, a Microsoft company. In this role for the past 12 years, Beranek has brought Nuance to a leadership position in the biometric authentication and biometric fraud prevention space. A thought leader in the field of biometrics, Beranek is a frequent contributor in industry events and the media on the topic of AI technology and it's use by the fraud community, and how society can mitigate against these evolving threats. Prior to Nuance, he held various leadership positions in the biometrics and security industry. He has earned a Bachelor of Commerce, Information Systems Major, from McGill University as well as an Executive Marketing certificate from Massachusetts Institute of Technology's Sloan School of Management. Beranek is also a certified Master Fraud Prevention Black Belt professional.

View all posts by Brett Beranek