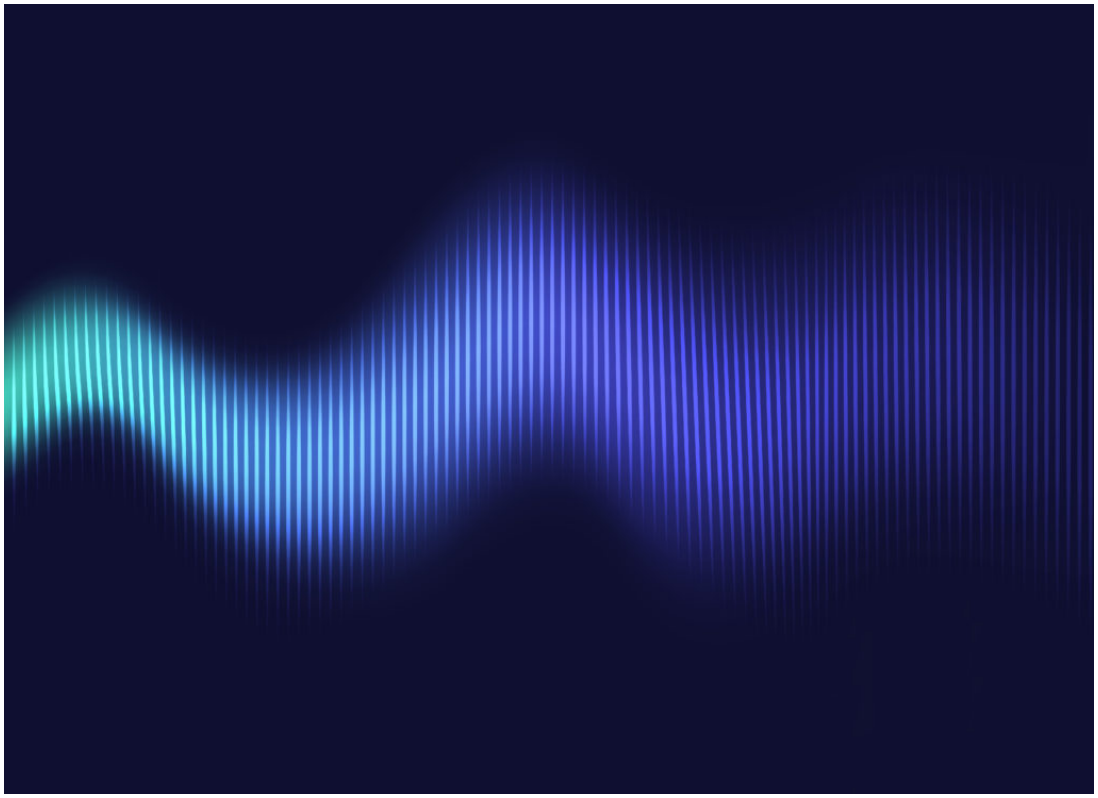
NUANCE | WHAT'S NEXT BLOG

Customer engagement, Authentication & fraud prevention

How Gatekeeper biometric authentication detects and beats synthetic voices

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

February 13, 2023



A new wave of text-to-speech AI is set to transform the security landscape. Here's how Nuance's biometric security innovations combine to provide the most effective protection against synthetic voice attacks—with a 99% detection rate for synthetic speech.

The rapid advancements in AI we've seen over the last few months are sending shockwaves through many industries, as leaders try to sift through the hype to understand the true future impact of emerging technologies. For many security professionals, the development of AI models that can generate synthetic voices using short samples of source audio has raised concerns about the efficacy of biometric authentication.

A seismic shift in the security landscape

Until now, synthetic voice attacks have been rare, due to the difficulty of creating usable voices with readily available tools. For fraudsters, it's been cheaper, faster, and easier to use other attack methods.

The latest speech synthesis models are still at the research stage and being developed responsibly with strong governance frameworks. However, there's no doubt that similar technology will eventually get into the hands of bad actors. And when synthetic voice generation becomes simple, fast, and cheap, we'll likely

see a shift in fraud tactics along with a new class of threats.

As fraudsters will deploy a new generation of deepfakes to circumvent biometric authentication mechanisms. The good news is, we'll be waiting for them—because Nuance has been preparing for these threats long before they made headlines.

Cutting-edge biometric authentication beats next-gen synthetic voices

At Nuance, we know we can't rest on our laurels, and fraudsters will continually look for ways to get around our security technologies. That's why we devote a huge amount of R&D effort into anticipating criminals' next steps and constantly staying one step ahead.

This "never stand still" mindset led us to release our first synthetic speech detection (SSD) algorithm back in 2014, long before fraudsters had meaningful access to the necessary technology for artificially creating voices. This algorithm detects the tiny differences that distinguish a computer-generated voice from a live human voice.

Since then, we've continuously optimized the SSD algorithm we use in Nuance Gatekeeper—our omnichannel biometric security solution—to improve its detection rate. And over the past year, we've joined forces with the Microsoft Cognitive AI research team to finetune our SSD capabilities, increasing the algorithm's detection rate to 86%.

What about the remaining 14%?

Well, that's where conversational biometrics comes in.

ConversationPrint is the latest innovative feature in Gatekeeper, adding an entirely new biometrics modality to our security capabilities. It analyzes the way people use language—including their word choices, grammar, sentence structure, and many other factors—and compares it to the conversational patterns of known customers.

So, even if fraudsters can synthesize a legitimate customer's voice, they still need to replicate their conversation pattern. That's extremely difficult to accomplish—especially if you only have a tiny amount of source audio to work with. The combination of voice biometrics, SSD, and ConversationPrint takes Gatekeeper's synthetic voice detection rate to 99%, giving our customers the most effective countermeasure against emerging AI-powered fraud attacks.

The war against fraud never stops—but each battle can be won

We can't stop criminals from getting their hands on sophisticated AI technologies. But we can prevent them from using those technologies to attack our customers and the people they serve. We'll continue to prioritize the optimization of our SSD algorithm to make life even harder for fraudsters. And we'll keep looking ahead to what they might try next, so we can neutralize future threats before they happen.

Tags: Nuance Gatekeeper, Synthetic voice detection, Deepfakes

More Information

Meet Nuance Gatekeeper

Find out how you can protect your customers and your business—whatever fraudsters try next.

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