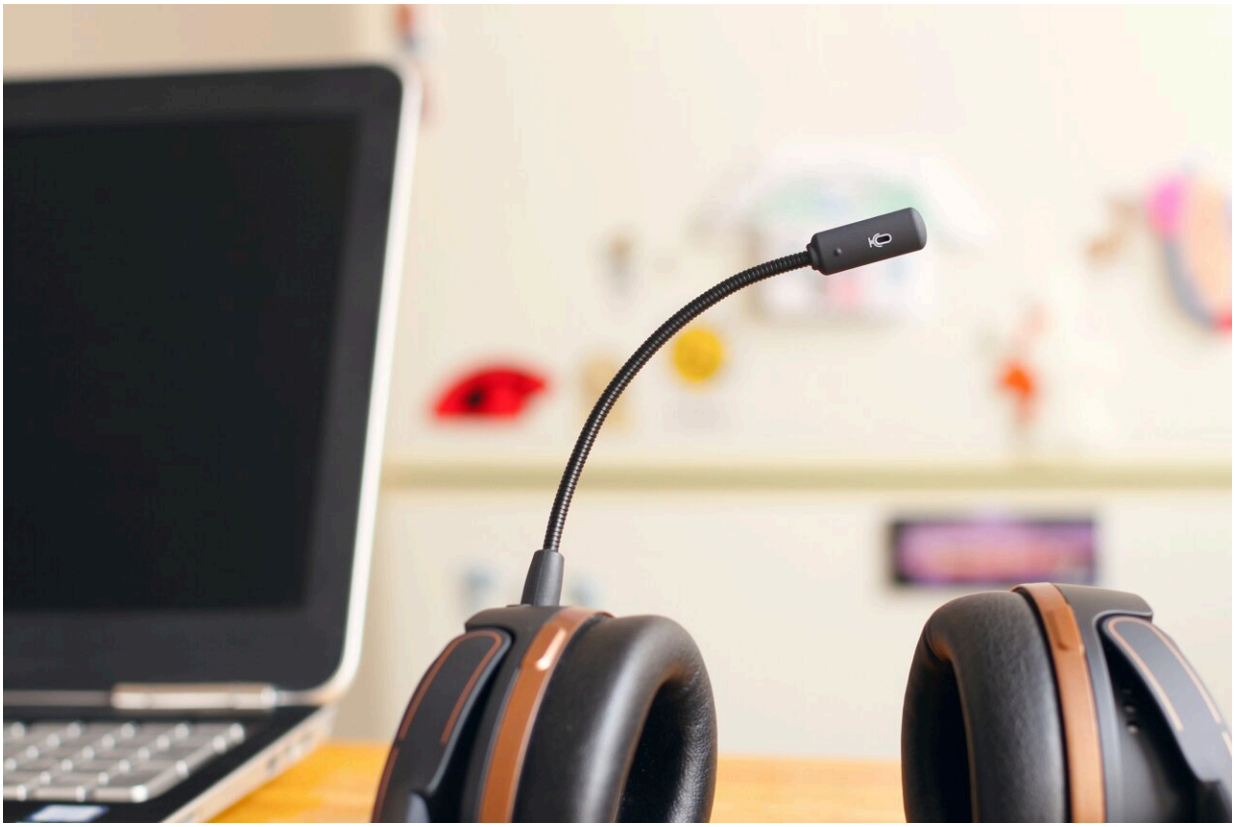
Attackers can break voice authentication with up to 99% success within six tries: Study

June 27 2023



Credit: Unsplash/CC0 Public Domain

Computer scientists at the University of Waterloo have discovered a method of attack that can successfully bypass voice authentication

security systems with up to a 99% success rate after only six tries.

Voice authentication—which allows companies to verify the identity of their clients via a supposedly unique "voiceprint"—has increasingly been used in remote banking, call centers and other security-critical scenarios.

"When enrolling in voice authentication, you are asked to repeat a certain phrase in your own voice. The system then extracts a unique vocal signature (voiceprint) from this provided phrase and stores it on a server," said Andre Kassis, a Computer Security and Privacy Ph.D. candidate and the lead author of a study detailing the research.

"For future authentication attempts, you are asked to repeat a different phrase and the features extracted from it are compared to the voiceprint you have saved in the system to determine whether access should be granted."

After the concept of voiceprints was introduced, malicious actors quickly realized they could use machine learning-enabled "deepfake" software to generate convincing copies of a victim's voice using as little as five minutes of recorded audio.

In response, developers introduced "spoofing countermeasures"—checks that could examine a speech sample and determine whether it was created by a human or a machine.

The Waterloo researchers have developed a method that evades spoofing countermeasures and can fool most voice authentication systems within six attempts. They identified the markers in deepfake audio that betray it is computer-generated, and wrote a program that removes these markers, making it indistinguishable from authentic audio.

In a recent test against Amazon Connect's voice authentication system,

they achieved a 10% success rate in one four-second attack, with this rate rising to over 40% in less than 30 seconds. With some of the less sophisticated voice authentication systems they targeted, they achieved a 99% success rate after six attempts.

Kassis contends that while voice authentication is obviously better than no additional security, the existing spoofing countermeasures are critically flawed.

"The only way to create a secure system is to think like an attacker. If you don't, then you're just waiting to be attacked," Kassis said.

Kassis' supervisor, computer science professor Urs Hengartner added, "By demonstrating the insecurity of voice authentication, we hope that companies relying on voice authentication as their only authentication factor will consider deploying additional or stronger authentication measures."

The research, Breaking Security-Critical Voice Authentication, by Kassis and Dr. Hengartner, was published in the proceedings of the 44th IEEE Symposium on Security and Privacy.

More information: Breaking Security-Critical Voice Authentication, 2023 IEEE Symposium on Security and Privacy (SP). DOI: 10.1109/SP46215.2023.00139 , www.computer.org/csdl/proceedi … 3600a951/1NrbYmtLXB6

Provided by University of Waterloo

authentication-success.html