Researcher Breaks reCAPTCHA With Google’s Speech-to-Text API

Researcher uses an old unCAPTCHA trick against latest the audio version of reCAPTCHA, with a 97 percent success rate.

An old attack method dating back to 2017 that uses voice-to-text to bypass CAPTCHA protections turns out to still work on Google’s latest reCAPTCHA v3.

That’s according to researcher Nikolai Tschacher, who posted a video proof-of-concept (PoC) of the attack on Jan. 2.

CAPTCHA, introduced in 2014, is an acronym for Completely Automated Public Turing Test to Tell Computers and Humans Apart. ReCaptcha is Google’s name for its own technology and free service that uses image, audio or text challenges to verify that a human is signing into an account. It’s a bit of code available free of charge from Google for accounts that handle less than 1 million queries a month. Google recently started charging for larger reCAPTCHA accounts.

“The idea of the attack is very simple: You grab the MP3 file of the audio reCAPTCHA and you submit it to Google’s own speech-to-text API,” Tschacher wrote. “Google will return the correct answer in over 97 percent of all cases.”

How does it work?

Everyone knows and hates reCAPTCHA. It looks like this:

The reCAPTCHA we all love

reCAPTCHA — an automated Turing Test.

The report includes a video showing how Tschacher's bot works. He added that this attack method works on even the latest version, reCAPTCHA v3.

Tschacher pointed out that his bot wouldn't be easy to exploit at scale for three specific reasons: Google rate-limits audio CAPTCHA access; Google is likely tracking bot metrics; and, it creates a fingerprint of each browsing device to stop bots.

"But still, we are approaching a point in time were the Turing Test can be solved by advanced AI, thus making CAPTCHAs harder and harder to implement," Tschacher told Threatpost. "CAPTCHAs will be replaced by passive AI that collects all kinds of data to constantly determine of the browsing signal appears to be human or not. The decision will be based on browsing fingerprint, JavaScript user interaction events such as mouse movements and key presses and IP-address metadata."

CAPTCHA, ReCAPTCHA, UnCAPTCHA

The idea of using speech-to-text against CAPTCHA protections was first introduced in 2017 by researchers at the University of Maryland, who then reported they "achieved 85 percent accuracy" with the tech they dubbed "UnCAPTCHA."

They explained that reCAPTCHA was designed to block Selenium browser automation engines, while, "unCAPTCHA2 uses a screen clicker to move to certain pixels on the screen and move around the page like a human," the researchers continued. "There is certainly work to be done here — the coordinates need to be updated for each new user and is not the most robust."

The report added that the reCAPTCHA bug was reported to Google in June 2018, and they okayed the release of the unCAPTCHA2 code.

"UnCAPTCHA2, like the original version, is meant to be a PoC," the report's disclaimer said. "As Google updates its service, this repository will *not* be updated. As a result, it is not expected to work in the future, and is likely to break at any time."

Now Tschacher appears to have come up with what could be called unCAPTCHA3, except now he said he can achieve a 97 percent success rate, instead of the original 85 percent reported in 2017.

Is CAPTCHA Secure?

"There has always been a game of cat-and-mouse between barriers like CAPTCHA and reCAPTCHA, and workarounds that attackers seeking automation employ," Oliver Tavakoli, Vectra CTO, told Threatpost. "This is a clever approach in that it uses an alternate scheme made available for visually impaired people to de-fang reCAPTCHA – and using Google's own speech-to-text API adds a bit of irony to the workaround. Hard to see how to supply support for the visually impaired without making reCAPTCHA a lot more easy to game."

But according to Dirk Schrader, global vice president with New Net Technoloiges, there isn't a ready replacement for widespread replacement of CAPTCHAs and that even if there was an easy swap to be made, the reality is that no single technology can replace good cybersecurity controls.

He added that CAPTCHA has been a reliable tool in separating machines from humans and might just need a bit of tweaking to keep up.

“The fact that one Google ‘machine’ is used against the other just adds the fun factor to the story,” Schrader said. “CAPTCHA has long been seen as a pain, however so far has proven to be a fairly good instrument to distinct human from machine interaction.”

https://threatpost.com/researcher-breaks-recaptcha-speech-to-text-api/162734/

https://www.itpro.com/security/cyber-security/358234/researcher-breaks-google-captcha-using-an-old-trick