Ten Eerste

2 min.

'Klik op alle gele taxi's': Computer doet zich perfect voor als mens in beruchte captcha-test

Om mensen van computers te onderscheiden bedachten beveiligingsonderzoekers ooit de captcha-puzzels voor websites. Bezoekers kregen pas na het aanklikken van de juiste plaatjes toegang tot een site. AI beheerst het trucje nu perfect.

LAURENS VERHAGEN

Onderzoekers van de ETH Zürich ontwikkelden een AI-model speciaal voor captcha's. Vergelijkbare pogingen bestaan al veel langer, maar voor het eerst is het succespercentage van de test nu 100 procent. Dit wil zeggen dat het AI-model in alle gevallen de computer aan de andere kant van de lijn voor de gek kan houden door zich voor te doen als mens. Net als mensen kan AI daar overigens wel meerdere pogingen voor nodig hebben.

Het achterliggende idee achter de zogenoemde captcha (Completely Automated Public Turing test to tell Computers and Humans Apart) was jaren geleden om geautomatiseerde software te weren van sites. Bijvoorbeeld bots die met gelekte inloggegevens proberen in te loggen.

Mensen kunnen de puzzels oplossen, computers niet, was lang de aanname. De eerste versies van de puzzels zagen er trouwens heel anders uit. Bezoekers zagen dan zwevende letters in vage vormen in een plaatje en moesten de juiste letters overtikken.

De variant met de verschillende plaatjes is het beruchtst onder internetters. Deze was immers niet alleen voor AI lastig op te lossen, maar óók voor mensen. Het enige wat nóg deprimerender is dan tegenover een computer je menselijkheid te moeten bewijzen? Daarin falen.

De grote vraag is nu wat de Zwitserse doorbraak in de praktijk betekent voor websites. Google, die de nu gekraakte variant ooit ontwikkelde, toont zich tegenover New Scientist niet in paniek. Google zegt dat de beperkingen van het mens-machine-onderscheid via het herkennen van plaatjes al langer bekend zijn.

Google ontwikkelde daarom jaren geleden een nieuw soort test, reCAPTCHA genaamd. In plaats van visuele testjes gebruikt het techbedrijf andere methoden om mens van machine te onderscheiden, zoals muisbewegingen. Tegenwoordig

zien veel websitebezoekers daarom de variant waarbij ze een vinkje moeten zetten bij het vakje 'Ik ben geen robot'.

Het goede nieuws is dat de irritante plaatjespuzzels met de brandkranen, zebrapaden en verkeerslichten geleidelijk zullen verdwijnen. Tenzij ze in omgekeerde vorm terugkeren: als de puzzel te goed wordt opgelost, is er vermoedelijk AI in het spel.