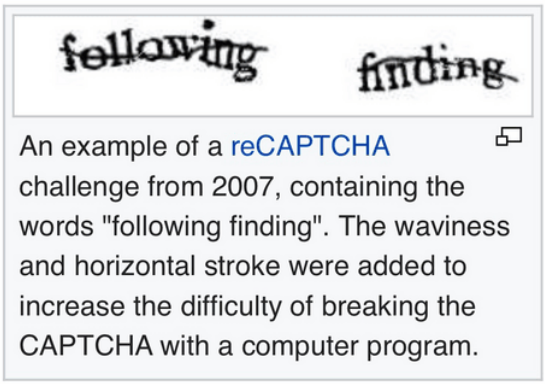
CAPTCHA-Alternative

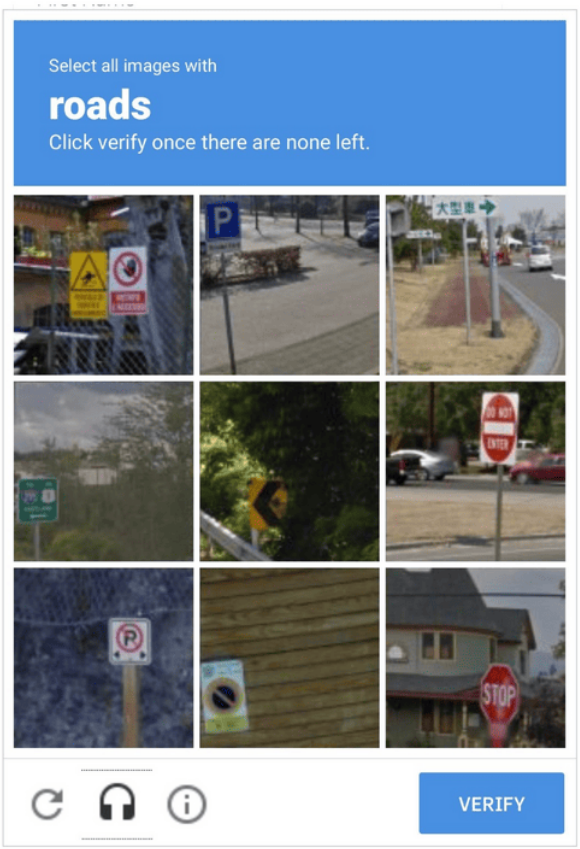
Schützen Sie Ihre Formulare benutzerfreundlich

Willem L. Middelkoop
July 30, 2022



An example of a reCAPTCHA challenge from 2007, containing the words "following finding". The waviness and horizontal stroke were added to increase the difficulty of breaking the CAPTCHA with a computer program.

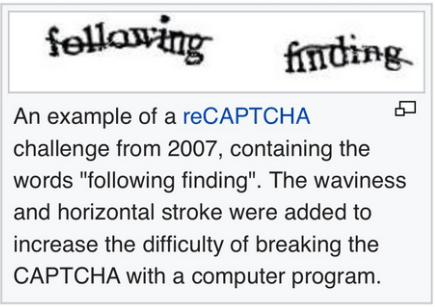
A CAPTCHA usually has a text box directly underneath where the user should fill out the text that they see. In this case, "sclt ..was here".



Wahrscheinlich sind Sie schon einmal einem CAPTCHA begegnet: Sie schützen Webformulare, indem sie Sie auffordern, seltsam gerenderte Zeichen abzutippen oder Fotos auszuwählen, die eine bestimmte Sache enthalten. Warum werden sie verwendet und gibt es eine benutzerfreundliche Alternative?

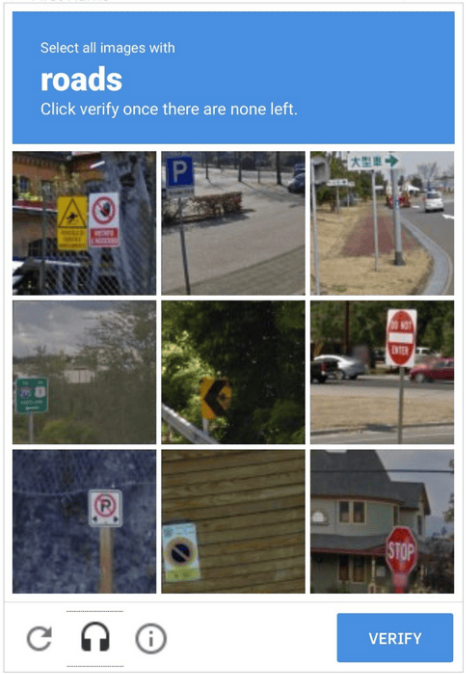
Was ist CAPTCHA?

CAPTCHA wurde entwickelt, um Computer und Menschen zu unterscheiden. CAPTCHAs erfordern oft, dass Sie etwas tun, was Computer nicht so einfach können. Daher steht das Akronym für: Completely Automated Public Turing test to tell Computers and Humans Apart. Webentwickler verwenden CAPTCHAs, um ihre Webformulare vor automatisiertem Spam und Missbrauch zu schützen.



An example of a reCAPTCHA challenge from 2007, containing the words "following finding". The waviness and horizontal stroke were added to increase the difficulty of breaking the CAPTCHA with a computer program.

A CAPTCHA usually has a text box directly underneath where the user should fill out the text that they see. In this case, "sclt ..was here".

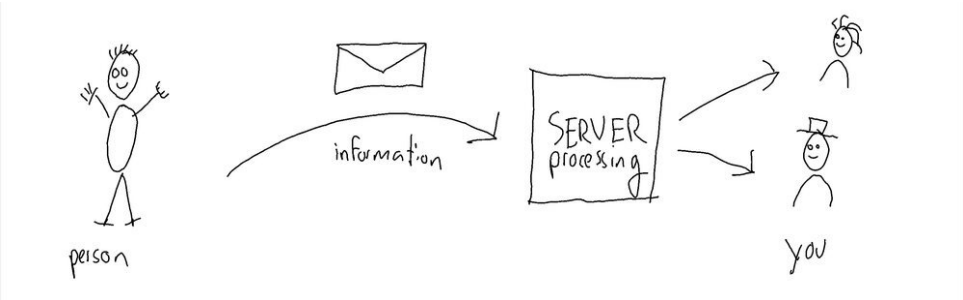


Typische CAPTCHAs, denen Sie im Internet begegnen können (Bildnachweis: Wikipedia und Google)

Warum benötigen Sie Formularschutz?

Ein typisches Webformular verwendet zwei Schritte:

- **Informationen eingeben:** Sie geben einige Informationen ein und klicken dann auf "ABSENDEN" (oder etwas Ähnliches), um fortzufahren.
- **Informationen verarbeiten:** Die von Ihnen eingegebenen Informationen werden von einem Server verarbeitet, der Ihre Nachricht oder Anfrage möglicherweise an die E-Mail-Adresse einer Person weiterleitet.



Ein typisches Webformular: Der Server verarbeitet Informationen von einer Person und leitet sie an andere Personen, wie Sie, weiter. Böswillige Akteure können den Absender leicht vortäuschen und so einen automatisierten Missbrauch Ihres Verarbeitungsservers ermöglichen.

Das Problem bei diesem typischen Ansatz ist, dass der erste Schritt leicht von böswilligen Akteuren automatisiert werden kann. Sie verwenden einen anderen Computer, um

wiederholt Informationen an den Server zu senden, wodurch dieser gezwungen wird, große Mengen an Informationen zu verarbeiten, die oft Spam-Nachrichten enthalten. Hacker sind besonders daran interessiert, Webformulare zu finden, bei denen sie die "AN"-Adresse manipulieren können, da sie dann Ihren Server verwenden können, um Spam-Nachrichten an beliebige Personen weltweit zu senden.

Ein CAPTCHA schützt Ihr Formular, indem es einen Computer daran hindert, automatisch Informationen an Ihren Server zu senden.

Probleme mit CAPTCHA

Ehrlich gesagt finde ich sie hässlich und umständlich, und ich bin nicht allein. Sie stellen eine Schwelle für Menschen dar: Sie senken die Konversionsraten, Klickraten usw. Außerdem sind sie oft sehr unfreundlich zu Menschen mit eingeschränktem Sehvermögen.

Kritiker beklagen sich auch darüber, dass Google einer der beliebtesten Anbieter von kostenlosen CAPTCHA-Tests ist. Man kann sich fragen, warum sie einen solchen Dienst kostenlos anbieten? Es ist eine ausgezeichnete Möglichkeit für sie, in den Kreislauf vieler (kommerzieller) Customer Journeys zu gelangen und ihre Algorithmen mit mehr Daten zur Profilerstellung von Personen zu füttern. Es ist etwas, das man bedenken sollte, wenn man Wert auf Datenschutz und DSGVO/Cookie-Gesetze legt.

Alternative

Deshalb habe ich mich daran gemacht, eine effektive Alternative zu CAPTCHAs zu entwickeln, die in den Webformularen verwendet werden kann, die ich für meine Kunden erstelle. Mein Ansatz ist zweistufig:

- **verstecken:** Die meisten böswilligen Akteure suchen nach möglichen Zielen, indem sie nach dem FORM-Tag suchen, das häufig zum Erstellen von Webformularen verwendet wird. Meine Formulare haben kein FORM-Tag, sondern verwenden andere gängige Elemente wie DIV: eine perfekte Tarnung. Wenn sie es nicht finden können, können sie es nicht knacken.
- **härten:** Meine Webformulare verwenden einen zusätzlichen Schritt, um den Missbrauch zu erschweren. Ich nenne es "eine Briefmarke besorgen" vor dem Absenden.

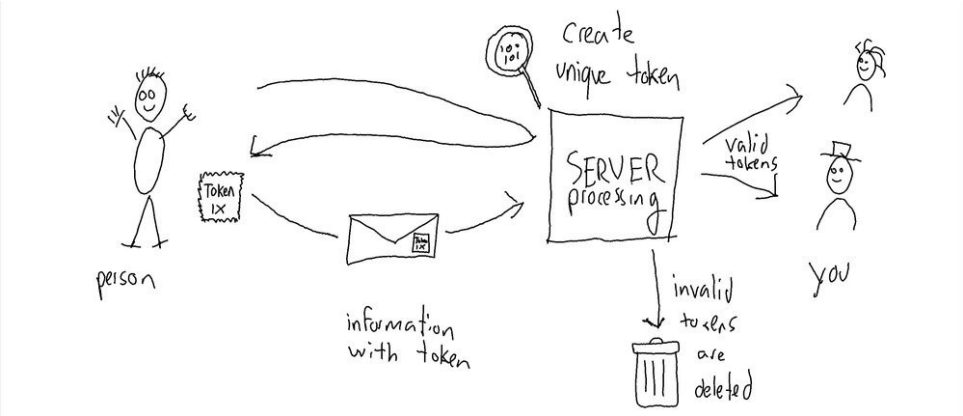
Kryptografische Signatur vor dem Absenden: die Briefmarke

Sie müssen verstehen, dass böswillige Akteure wirtschaftlich denken: Sie werden sich nur so viel Mühe geben, wie der potenzielle Gewinn wert ist. Wenn Sie es ihnen schwer genug machen, Ihr Webformular zu missbrauchen, ist die Wahrscheinlichkeit groß, dass sie weiterziehen und es dabei belassen. Bevor ich erkläre, was ich getan habe, muss ich Sie warnen:

Haftungsausschluss: *Sie müssen das Ziel Ihres Formularschutzes berücksichtigen, in meinem Fall ist es die (starke) Reduzierung der Anzahl von Spam-Nachrichten bei gleichzeitiger Wahrung der Benutzerfreundlichkeit. Dies erlaubt es mir, ein System zu entwickeln, das nicht unbedingt einen "bombensicheren" Schutz bietet, aber wenn Sie versuchen, Atomgeheimnisse zu schützen, ist dieser Ansatz möglicherweise nicht für Sie geeignet. Berücksichtigen Sie immer Ihr Bedrohungsmodell!*

Um Webformulare zu schützen, führe ich einen zusätzlichen Schritt ein, den ich "Briefmarke besorgen" nenne. Die Schritte des geschützten Webformulars sehen dann wie folgt aus:

- **Informationen eingeben:** Sie geben einige Informationen ein und klicken dann auf "ABSENDEN" (oder etwas Ähnliches), um fortzufahren.
- **Briefmarke besorgen:** Kurz bevor die eigentlichen Informationen abgeschickt werden, kontaktiert Ihr Gerät den Server, um ein kryptografisches Token anzufordern, das den Eigenschaften der eigentlichen Informationen *und* des Absenders entspricht. Dies geschieht in Millisekunden, die Leute werden es nicht bemerken. Stellen Sie sich das Token als eine Briefmarke vor, die speziell für das Paket gedacht ist, das Sie versenden - und nur einmal verwendet werden kann.
- **Informationen verarbeiten:** Die von Ihnen eingegebenen Informationen werden mit dem kryptografischen Token kombiniert und an den Server gesendet. Wenn das Token gültig ist, werden die Informationen wie gewohnt verarbeitet. Ungültige Token werden einfach ignoriert, was wichtig ist, um Reverse Engineering sehr schwierig zu machen, indem kein Feedback gegeben wird (der Server sagt immer "OK" :-))!



Durch die Einführung eines eindeutigen, nur einmal verwendbaren Tokens für jede Nachricht wird es für böswillige Akteure viel schwieriger, den Prozess des Versendens von Nachrichten zu automatisieren - und schützt so Ihr Formular vor Spammern.

Seit 2016 verwende ich diesen Ansatz und die Post-Processing-Server haben buchstäblich Millionen von Nachrichten verarbeitet, wobei extrem wenige Nachrichten (<100) Spam waren. Bei näherer Betrachtung ist der größte Teil des Spams, der durchkommt, "Handarbeit": möglicherweise ein Hinweis darauf, dass böswillige Akteure den Mechanismus untersuchen. Da es offenbar zu mühsam ist, das System zu knacken, ist es sehr effektiv, um mein Ziel zu erreichen, die Webformulare zu schützen.

Fazit

Obwohl CAPTCHAs verständlicherweise sehr beliebt sind, ist es nicht immer notwendig, sie in Ihren Webformularen zu verwenden, wenn Sie Alternativen in Betracht ziehen. Mein Rat ist, es böswilligen Akteuren schwerer und Ihrem Publikum leichter zu machen!