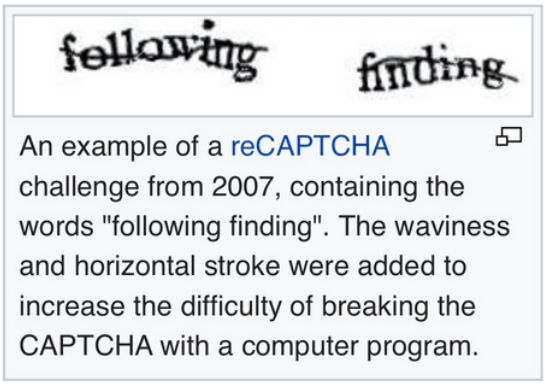
Alternativa a CAPTCHA

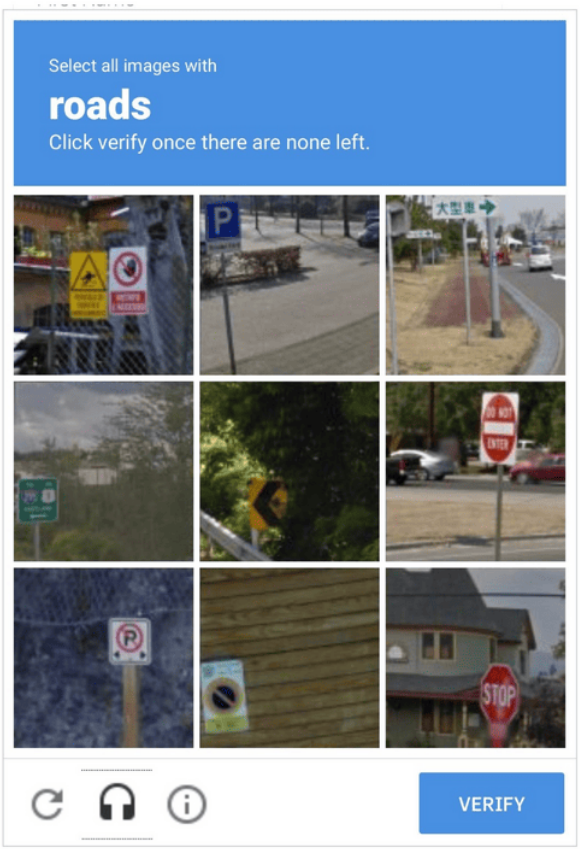
Proteja sus formularios de forma fácil para el usuario

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.

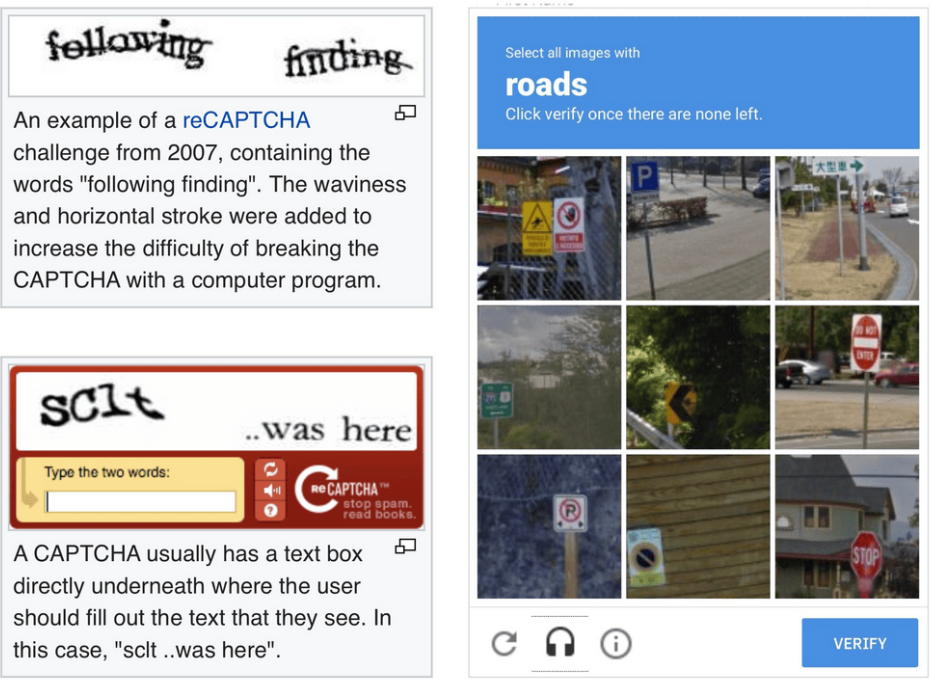
A CAPTCHA usually has a text box directly underneath where the user should fill out the text that they see. In this case, "sclt ..was here".



Es probable que te hayas encontrado con un CAPTCHA: protegen los formularios web pidiéndote que escribas caracteres con una representación extraña o que selecciones fotos que contengan un elemento en particular. ¿Por qué se utilizan y existe una alternativa fácil de usar?

¿Qué es CAPTCHA?

Diseñado para diferenciar entre computadoras y humanos, los CAPTCHA a menudo requieren que hagas algo que las computadoras no pueden hacer fácilmente. De ahí que el acrónimo signifique: Prueba de Turing Pública Completamente Automatizada para diferenciar Computadoras y Humanos. Los creadores web utilizan CAPTCHA para proteger sus formularios web contra el spam automatizado y el abuso.

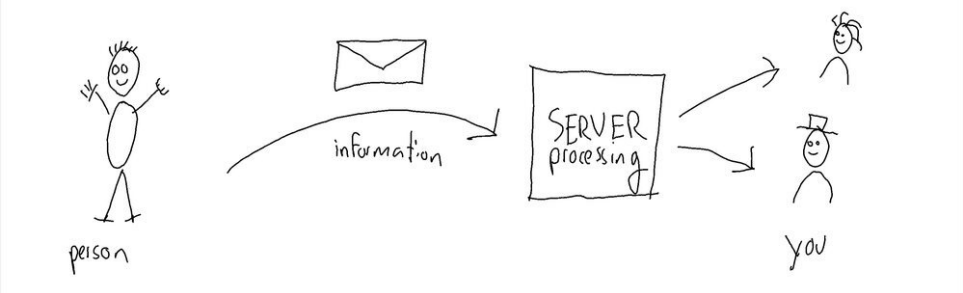


CAPTCHA típicos que puede encontrar en la web (crédito de la imagen: Wikipedia y Google)

¿Por qué necesitas protección de formularios?

Un formulario web típico utiliza dos pasos:

- **ingresar información:** Ingresas información y luego haces clic en ”ENVIAR” (o algo similar) para continuar.
- **procesar información:** La información que ingresaste es procesada por un servidor, posiblemente reenviando tu mensaje o solicitud al correo electrónico de alguien.



Un formulario web típico: el servidor procesa la información de una persona, enviándola a otras personas, como usted. Los actores maliciosos pueden falsificar fácilmente a la persona que envía, lo que permite el abuso automatizado de su servidor de procesamiento.

El problema con este enfoque típico es que el primer paso puede ser fácilmente automatizado por actores maliciosos. Utilizan otra computadora para enviar repetidamente información al servidor, obligándolo a procesar mucha información, que a menudo contiene

mensajes de spam. Los hackers están especialmente interesados en encontrar formularios web donde puedan manipular la dirección "PARA", porque entonces pueden usar tu servidor para enviar mensajes de spam a cualquier persona en el mundo.

Un CAPTCHA protege tu formulario al impedir que una computadora envíe automáticamente información a tu servidor.

Problemas con CAPTCHA

Francamente, creo que son feos y engorrosos, y no estoy solo. Introducen un umbral para las personas: reduciendo las tasas de conversión, las tasas de clics, etc. Además, a menudo son muy poco amigables para las personas con problemas de visión.

Los críticos también se quejan de que Google es uno de los proveedores más populares de pruebas CAPTCHA gratuitas. Uno puede preguntarse ¿por qué ofrecen tal servicio de forma gratuita? Es una excelente manera para ellos de entrar en el bucle de muchos viajes de clientes (comerciales), alimentando sus algoritmos con más datos para perfilar a las personas. Es algo a considerar si valoras la privacidad y las leyes de GPDR/cookies.

Alternativa

Es por eso que me propuse crear una alternativa efectiva para los CAPTCHA que se utilizarán en los formularios web que construyo para mis clientes. Mi enfoque es doble:

- **ocultar:** la mayoría de los actores maliciosos buscan posibles objetivos buscando cualquier etiqueta FORM, que a menudo se utiliza para crear formularios web. Mis formularios no tienen la etiqueta FORM, sino que utilizan otros elementos comunes como DIV: creando un camuflaje perfecto. Si no pueden verlo, no pueden romperlo.
- **reforzar:** mis formularios web utilizan un paso adicional para dificultar la automatización de su abuso. Lo llamo "obtener un sello postal" antes de enviar.

Firma criptográfica previa al envío: el sello postal

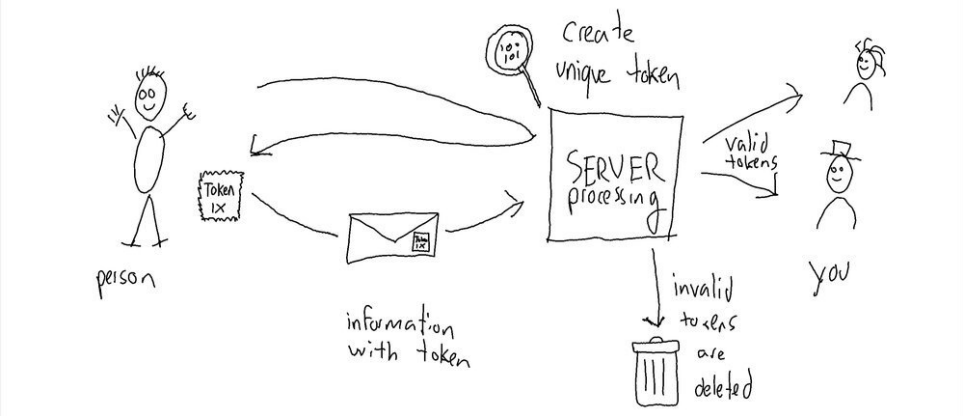
Debes comprender que los actores maliciosos piensan económicamente: solo harán un esfuerzo si la ganancia potencial lo vale. Si les dificultas el abuso de tu formulario web, es probable que sigan adelante y lo dejen. Antes de explicar lo que hice, debo advertirte:

Descargo de responsabilidad: *Debes considerar el objetivo de la protección de tu formulario, en mi caso es (en gran medida) reducir la cantidad de mensajes de spam preservando la facilidad de uso. Esto me permite pensar en un sistema que no necesariamente proporciona una protección "a prueba de bombas", sin embargo, si estás tratando de proteger secretos nucleares, entonces este enfoque podría no ser adecuado para ti. ¡Siempre considera tu modelo de amenaza!*

Para proteger los formularios web, introduzco un paso adicional que denominé "obtener un sello postal". Los pasos del formulario web protegido se convierten en:

- **ingresar información:** Ingresas información y luego haces clic en "ENVIAR" (o algo similar) para continuar.
- **obtener sello postal:** Justo antes de que se envíe la información real, tu dispositivo se comunica con el servidor para solicitar un token criptográfico que coincida con las características de la información real *y* el remitente. Esto sucede en milisegundos, la gente no lo notará. Piensa en el token como un sello postal, específico para el paquete que estás enviando, que se utilizará solo una vez.

- **procesar información:** La información que ingresaste se combina con el token criptográfico y se envía al servidor. Si el token es válido, la información se procesa como de costumbre. Los tokens inválidos simplemente se ignoran, lo cual es importante para dificultar mucho la ingeniería inversa al no proporcionar ningún comentario (¡el servidor siempre dice "OK" :-))!



Al introducir un token único, de un solo uso, para cada mensaje, se hace mucho más difícil para los actores maliciosos automatizar el proceso de envío de mensajes, protegiendo su formulario contra los spammers.

Desde 2016 he estado ejecutando este enfoque y los servidores de posprocesamiento han manejado literalmente millones de mensajes, con muy pocos mensajes (<100) siendo spam. Tras una inspección más detallada, la mayor parte del spam que pasa es "trabajo manual": posiblemente indica que los actores maliciosos están investigando el mecanismo. Como parece ser demasiado esfuerzo romper el sistema, es muy efectivo para lograr mi objetivo de proteger los formularios web.

Conclusión

Si bien los CAPTCHA son comprensiblemente muy populares, no siempre es necesario tenerlos en tus formularios web si consideras alternativas. ¡Mi consejo es dificultarles las cosas a los actores maliciosos y facilitarlas a tu audiencia!