

## Do CAPTCHA ao reCAPTCHA ou um caso feliz de cooperação entre homem e máquina<sup>1</sup>

Ora bem, comecemos pelo mais elementar. O que é um CAPTCHA? Num universo globalizado e potencialmente opaco como é o da *World Wide Web*, os responsáveis pela segurança dos sites tiveram de criar formas de impedir que programas automatizados (chamados *bots*) se introduzissem nos serviços disponibilizados *on-line* e operassem acções ilícitas ou abusivas. Um CAPTCHA, ao contrário do que o nome possa sugerir, como se se tratasse de algo de complexo e ininteligível, é simplesmente uma forma de evitar que estas intromissões tomem lugar.

Mas se um CAPTCHA é, afinal, uma realidade facilmente apreensível, por que motivo tem um nome aparentemente tão estranho? É que, apesar de ser pronunciável, não deixa de ser uma sigla, com tudo o que as siglas podem ter de estranho e original. CAPTCHA significa, pois, ***Completely Automated Public Turing test to tell Computers and Humans Apart***, que, em português, poderíamos traduzir como *Teste Público Completamente Automatizado para Distinguir entre Humanos e Computadores*.

Tão simples como perceber o que fazem os CAPTCHA, é reconhecê-los. A maior parte dos cibernautas já os viu ou utilizou. Um CAPTCHA típico é formado por uma imagem com caracteres distorcidos e parcialmente rasurados que, regra geral, aparece no rodapé das páginas de registo de um serviço. Aos utilizadores, é pedido que reproduzam, num espaço em branco, os tais caracteres distorcidos, pois é isso que prova que o utilizador é humano e não um computador. De facto, os programas de computadores não conseguem ler e interpretar texto distorcido de uma forma tão eficaz como os seres humanos, daí que os CAPTCHAs sejam utilizados para impedir que esses programas se infiltrem maliciosamente em serviços *on-line*, como, por exemplo, serviços de correio gratuito ou venda de bilhetes, com o intuito de se obterem endereços de correio para acções de spam ou de se comprarem largas quantidades de bilhetes que são vendidos, mais tarde, a preços inflacionados.

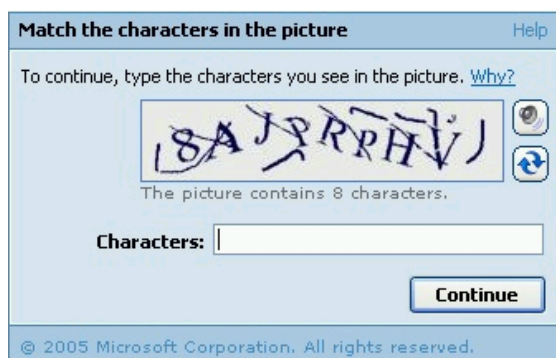


Fig. 1 - Exemplo de um CAPTCHA

<sup>1</sup> Com base no documento "reCAPTCHA: Human-Based Character Recognition via Web Security Measures", publicado em 12 de Setembro de 2008 na página [www.sciencemag.org](http://www.sciencemag.org).

Estima-se que, todos os dias, sejam reproduzidos mais de 100 milhões de CAPTCHAs, em operações que não demoram mais do que alguns segundos, se bem que, no seu conjunto, representem milhares de horas despendidas pelos utilizadores humanos num esforço mental circunscrito e concreto. Bem explorado, esse esforço não poderia ser utilizado para outros fins? Alguém se lembrou, pois, de aproveitar uma acção que já era feita milhões de vezes por dia para realizar outras tarefas, as quais, se tivessem de ser realizadas de propósito, implicariam tais custos e tempo que estariam fadadas ao insucesso. Mais portuguesmente, a ideia foi “matar dois coelhos de uma cajadada só”. Como assim?

A Escola de Ciências da Computação, da Universidade de Carnegie Mellon, em Pittsburgh, nos Estados Unidos da América, teve a ideia de usar CAPTCHAs para ajudar a tarefa de digitalização de textos tipografados em suporte papel. Actualmente, esse tipo de textos está a ser digitalizado em massa, com o objectivo evidente de preservar a memória histórica e de a tornar acessível à escala planetária. Os textos, depois de digitalizados, resultam em imagens que, de seguida, são convertidas em ficheiros de texto através de programas de reconhecimento óptico de caracteres (OCR). Qual a vantagem de converter as imagens em texto? É que o texto, ao contrário do conteúdo “textual” de uma imagem, pode ser facilmente indexado e pesquisado, o que aumenta extraordinariamente as possibilidades de recuperação de informação. Ao mesmo tempo, os ficheiros de texto são mais “leves” do que as imagens e, ao invés destas, editáveis. Mas, no maravilhoso mundo em que vivemos, ainda não há belas sem senão...

Acontece, pois, que o reconhecimento óptico de caracteres é falível quando se trata de decifrar as palavras dos documentos digitalizados. Sabe-se, por exemplo, que o OCR reconhece apenas 20% das palavras que tenham sido digitalizadas a partir de documentos amarelecidos e com texto esbatido. Num significativo contraste, duas pessoas, utilizando a técnica de escrever e verificar (“key and verify”), segundo a qual cada pessoa escreve o texto independentemente e, depois, identificam as diferenças entre os registos, podem atingir uma precisão de 99%, embora esta solução seja demasiado dispendiosa e, por isso, só aplicada a documentos de grande importância.

Há alguma solução de recurso?

Sim. A Escola de Ciências da Computação da Universidade de Carnegie Mellon encontrou nos CAPTCHAs a forma mais rápida e viável de contornar as dificuldades manifestadas pelo reconhecimento óptico de caracteres inscritos em imagens e de contribuir assim para tornar mais eficazes a digitalização e disponibilização de enormes massas documentais de relevância histórica. Para o efeito, adaptou a solução dos CAPTCHAs, rebaptizando-a de “reCAPTCHA”. O seu funcionamento é em tudo semelhante aos dos CAPTCHAs, ainda que com algumas nuances e particularidades. Enquanto que os CAPTCHAs são imagens representando uma sequência aleatória de caracteres criada por um computador, o reCAPTCHA apresenta ao utilizador palavras retiradas de documentos digitalizados que não foram devidamente identificadas pelos programas de reconhecimento óptico de caracteres. Ora, ao pedir-se ao

utilizador que reproduza estas palavras, como se de um CAPTCHA se tratasse, garante-se que as mesmas vão ser, com grande probabilidade, decifradas, mas, ao mesmo tempo, o processo tem de garantir que os objectivos dos CAPTCHA são igualmente cumpridos. Como é que funciona este esquema?

O reCAPTCHA dá ao utilizador duas palavras. Uma delas é a chamada “palavra desconhecida”; a outra, a “palavra de controlo”, já conhecida pelo sistema e apresentada aleatoriamente, de modo a diminuir a probabilidade de os programas automáticos a decifrarem. Se o utilizador escrever correctamente a “palavra de controlo”, o sistema assume que esse utilizador é humano, esperando-se que escreva também correctamente a “palavra desconhecida”.

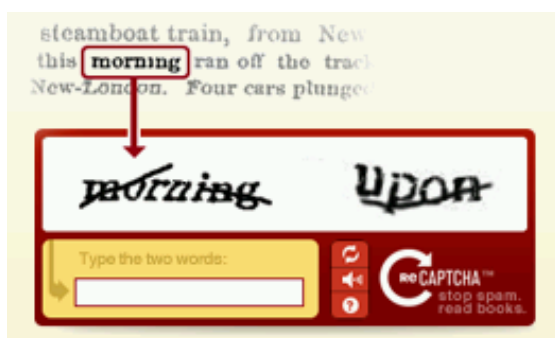


Fig. 2 - Exemplo de um reCAPTCHA

Agora, à semelhança dos programas de OCR, também os seres humanos podem errar na decifração das palavras desconhecidas. De modo a diminuir a margem de erro, o reCAPTCHA disponibiliza a mesma “palavra suspeita” (que não foi devidamente decifrada pela acção consertada de dois programas de OCR) a vários utilizadores, aos quais é apresentada como “palavra desconhecida” com diferentes distorções aleatórias, que impedem que seja lida por computadores e programas automáticos. A partir do momento em que o utilizador decifra a “palavra de controlo” associada, a sua resposta para a “palavra desconhecida” é gravada como um palpite plausível. Se os palpites dos três primeiros utilizadores coincidirem entre si e se forem diferentes das soluções dadas pelo programa de OCR, então – e só então – a resposta é dada como certa e transforma-se em “palavra de controlo” para futuros utilizadores. Quando existem discrepâncias entre as respostas humanas, o reCAPTCHA apresenta a “palavra desconhecida” a mais utilizadores e selecciona o palpite com o maior número de ocorrências ou votos, numa lógica em que cada resposta humana representa um voto e cada palpite do OCR meio voto. Um palpite deve colher, pelo menos, dois votos e meio antes de ser aceite como a decifração correcta da “palavra desconhecida”. Paralelamente, o reCAPTCHA também prevê a ocorrência de palavras que sejam ilegíveis, pelo que oferece ao utilizador a possibilidade de pedir um novo par de palavras. Quando seis utilizadores rejeitam a mesma palavra, esta é retirada como ilegível.

Uma implementação a larga escala do reCAPTCHA já permitiu chegar a algumas conclusões. A primeira delas é que este processo de decifração quase que iguala a performance dos serviços personalizados de transcrição.

Cinquenta artigos de jornal digitalizados, de cinco anos diferentes, foram escolhidos casualmente e transcritos por uma equipa de dois profissionais para testar a eficácia do reCAPTCHA. De um total de 24084 palavras, o reCAPTCHA não foi capaz de decifrar apenas 216, o que confere a este sistema uma eficácia de 99,1%. Esta percentagem, já de si elevada, ganha maior expressão se tomarmos em linha de conta que, por um lado, a eficácia do OCR se quedou pelos 83,5% e que, por outro, o standard mínimo de eficácia definido pela indústria para a técnica humana de escrever e verificar (“key and verify”) se situa nos 99%.

Numa segunda conclusão, confirma-se a viabilidade dos CAPTCHAs como forma de canalizar o mesmo esforço mental humano para fins diversos. Decorrido um ano de funcionamento do sistema, os utilizadores humanos, ao mesmo tempo que resolveram mais de 1,2 mil milhões de CAPTCHAs, decifraram mais de 440 milhões de palavras suspeitas, o que equivale a cerca de 17600 livros transcritos manualmente. E a crescente popularidade do sistema é tal que, em meados de 2008, a taxa de transcrição de palavras suspeitas era de 4 milhões por dia.

Há, assim, várias razões de peso para os sites adoptarem o sistema reCAPTCHA e os cibernautas utilizarem-no. Inversamente, não há nenhum motivo para o não fazerem. Se, por um lado, o reCAPTCHA promove a disponibilização digital de textos de relevância histórica a baixo custo, num menor intervalo de tempo, com maior qualidade e em doses maciças, por outro, garante maior segurança aos sites do que os CAPTCHAs convencionais, uma vez que estes são vulneráveis a programas ilícitos, ao invés das palavras apresentadas pelo reCAPTCHA, que são praticamente indecifráveis por computadores. Além disso, o tempo que um utilizador despende para decifrar um CAPTCHA convencional ou um reCAPTCHA é praticamente o mesmo.

Àqueles que necessitam de um mecanismo de controlo de registo nos seus sites, pergunta-se: do que é que estão à espera para aderir ao reCAPTCHA? A segurança na Web e a memória histórica, realidades que, à partida, ninguém esperava ver associadas, agradecem esse pequeno gesto, que dá tanto por tão pouco.

João Sabino  
Agosto de 2009