CAPTCHA

Test to determine whether a user is human / From Wikipedia, the free encyclopedia

DEAR WIKIWAND AI, LET'S KEEP IT SHORT BY SIMPLY ANSWERING THESE KEY QUESTIONS:

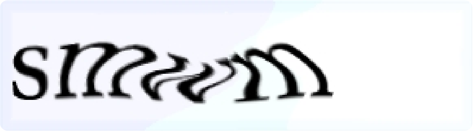
Can you list the top facts and stats about CAPTCHA?

Summarize this article for a 10 year old

SHOW ALL QUESTIONS

A **CAPTCHA** (/ˈkæp.tʃə/ *KAP-chə*) is a type of challenge–response test used in computing to determine whether the user is human in order to deter bot attacks and spam.[1]

The term was coined in 2003 by Luis von Ahn, Manuel Blum, Nicholas J. Hopper, and John Langford.[2] It is a contrived acronym for "Completely Automated Public Turing test to tell Computers and Humans Apart."[3] A historically common type of CAPTCHA (displayed as Version 1.0[*clarification needed*]) was first invented in 1997 by two groups working in parallel. This form of CAPTCHA requires entering a sequence of letters or numbers in a distorted image. Because the test is administered by a computer, in contrast to the standard Turing test that is administered by a human, CAPTCHAs are sometimes described as reverse Turing tests.[4]



This CAPTCHA (Version 1[*clarification needed*]) of "smwm" obscures its message from computer interpretation by twisting the letters and adding a slight background color gradient.

Two widely used CAPTCHA services are Google's reCAPTCHA[5] [6] and the independent hCaptcha.[7] [8] It takes the average person approximately 10 seconds to solve a typical CAPTCHA.[9]

Purpose

CAPTCHAs' purpose is to prevent spam on websites, such as promotion spam, registration spam, and data scraping, and bots are less likely to abuse websites with spamming if those websites use CAPTCHA. Many websites use CAPTCHA effectively to prevent bot raiding. CAPTCHAs are designed so that humans can complete them, while most robots cannot.[10] Newer CAPTCHAs look at the user's behaviour on the internet, to prove that they are a human.[11] A normal CAPTCHA test only appears if the user acts like a bot, such as when they request webpages, or click links too fast.

History

Since the 1980s–1990s, users have wanted to make text illegible to computers.[12] The first such people were hackers, posting about sensitive topics to Internet forums they thought were being automatically monitored on keywords. To circumvent such filters, they replaced a word with look-alike characters. *HELLO* could become `|-|3|_|_()` or `)-(3££0`, and others, such that a filter could not detect *all* of them. This later became known as leetspeak.[13]

One of the earliest commercial uses of CAPTCHAs was in the Gausebeck–Levchin test. In 2000, idrive.com began to protect its signup page[14] with a CAPTCHA and prepared to file a patent.[12] In 2001, PayPal used such tests as part of a fraud prevention strategy in which they asked humans to "retype distorted text that programs have difficulty recognizing."[15] PayPal co founder and CTO Max Levchin helped commercialize this use.

A popular deployment of CAPTCHA technology, reCAPTCHA, was acquired by Google in 2009.[16] In addition to preventing bot fraud for its users, Google used reCAPTCHA and CAPTCHA technology to digitize the archives of *The New York Times* and books from Google Books in 2011.[17]

Invention

Eran Reshef, Gili Raanan and Eilon Solan, who worked at Sanctum on Application Security Firewall, first patented CAPTCHA in 1997. Their patent application details that "The invention is based on applying human advantage in applying sensory and cognitive skills to solving simple problems that prove to be extremely hard for computer software. Such skills include, but are not limited to processing of sensory information such as identification of objects and letters within a noisy graphical environment, signals and speech within an auditory signal, patterns and objects within a video or animation sequence".[18]

Characteristics

CAPTCHAs are automated, requiring little human maintenance or intervention to administer, producing benefits in cost and reliability.[19]

Modern text-based CAPTCHAs are designed such that they require the simultaneous use of three separate abilities—invariant recognition, segmentation, and parsing to complete the task.[20]

- Invariant recognition refers to the ability to recognize letters despite a large amount of variation in their shapes.[21]
- Segmentation is the ability to separate one letter from another, made difficult in CAPTCHAs.
- Parsing refers to the ability to understand the CAPTCHA holistically, in order to correctly identify each character.[22]

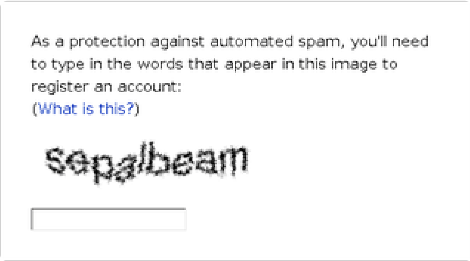
Each of these problems poses a significant challenge for a computer, even in isolation. Therefore, these three techniques in tandem make CAPTCHAs difficult for computers to solve.[23]

Whilst primarily used for security reasons, CAPTCHAs can also serve as a benchmark task for artificial intelligence technologies. According to an article by Ahn, Blum and Langford,[24] "any program that passes the tests generated by a CAPTCHA can be used to solve a hard unsolved AI problem."[25] They argue that the advantages of using hard AI problems as a means for security are twofold. Either the problem goes unsolved and there remains a reliable method for distinguishing humans from computers, or the problem is solved and a difficult AI problem is resolved along with it.[24]

Accessibility

See also: Web accessibility

CAPTCHAs based on reading text—or other visual-perception tasks—prevent blind or visually impaired users from accessing the protected resource.[26] However, CAPTCHAs do not have to be visual. Any hard artificial intelligence problem, such as speech recognition, can be used as CAPTCHA. Some implementations of CAPTCHAs permit users to opt for an audio CAPTCHA, such as reCAPTCHA, though a 2011 paper demonstrated a technique for defeating the popular schemes at the time.[27]



As a protection against automated spam, you'll need to type in the words that appear in this image to register an account:
(What is this?)

Many websites require typing a CAPTCHA when creating an account to prevent spam. This image contains a user trying to type the CAPTCHA word "sepalbeam" to protect against automated spam.

Blind or visually impaired people have problems with CAPTCHAs.[28] Because CAPTCHAs are designed to be unreadable by machines, common assistive technology tools such as screen readers cannot interpret them. Since sites may use CAPTCHAs as part of the initial registration process, or even every login, this challenge can block access. In certain jurisdictions, site owners could become targets of litigation if they are using CAPTCHAs that discriminate against certain people with disabilities. For example, a CAPTCHA may make a site incompatible with Section 508 in the United States.

The use of CAPTCHA thus excludes a small percentage of users from using significant subsets of such common Web-based services as PayPal, Gmail, Orkut, Yahoo!, many forum and weblog systems, etc.[29]

A method of improving CAPTCHA to ease the work with it was proposed by ProtectWebForm and named "Smart CAPTCHA".[30] Developers are advised to combine CAPTCHA with JavaScript. Since it is hard for most bots to parse and execute JavaScript, a combinatory method which fills the CAPTCHA fields and hides both the image and the field from human eyes was proposed.[31]

One alternative method involves displaying to the user a simple mathematical equation and requiring the user to enter the solution as verification. Although these are much easier to defeat using software, they are suitable for scenarios where graphical imagery is not appropriate, and they provide a much higher level of accessibility for blind users than the image-based CAPTCHAs. These are sometimes referred to as MAPTCHAs (M = "mathematical"). However, these may be difficult for users with a cognitive disorder, such as dyscalculia.[32]

Challenges such as a logic puzzle, or trivia question can also be used as a CAPTCHA. There is research into their resistance against countermeasures.[33]

Circumvention

Two main ways to bypass CAPTCHA include using cheap human labor to recognize them, and using machine learning to build an automated solver.[34] According to former Google "*click fraud czar*" Shuman Ghosemajumder, there are numerous services which solve CAPTCHAs automatically.[35]

Machine learning-based attacks

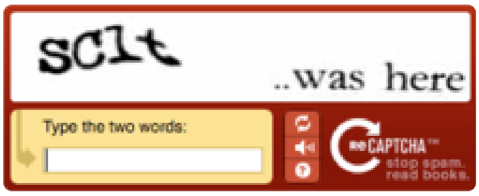
There was not a systematic methodology for designing or evaluating early CAPTCHAs.[23] As a result, there were many instances in which CAPTCHAs were of a fixed length and therefore automated tasks could be constructed to successfully make educated guesses about where segmentation should take place. Other early CAPTCHAs contained limited sets of words, which made the test much easier to game. Still others[*example needed*] made the mistake of relying too heavily on background confusion in the image. In each case, algorithms were created that were successfully able to complete the task by exploiting these design flaws. However, light changes to the CAPTCHA could thwart them. Modern CAPTCHAs like reCAPTCHA rely on present variations of characters that are collapsed together, making them hard to segment, and they have warded off automated tasks.[36]

In October 2013, artificial intelligence company Vicarious claimed that it had developed a generic CAPTCHA-solving algorithm that was able to solve modern CAPTCHAs with character recognition rates of up to 90%.[37] However, Luis von Ahn, a pioneer of early CAPTCHA and founder of reCAPTCHA, said: "It's hard for me to be impressed since I see these every few months." 50 similar claims to that of Vicarious had been made since 2003.[38]

following
finding

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.

In August 2014 at Usenix WoOT conference, Bursztein et al. presented the first generic CAPTCHA-solving algorithm based on reinforcement learning and demonstrated its efficiency against many popular CAPTCHA schemas.[36]



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".

In October 2018 at ACM CCS'18 conference, Ye et al. presented a deep learning-based attack that could consistently solve all 11 text captcha schemes used by the top-50 popular websites in 2018. An effective CAPTCHA solver can be trained using as few as 500 real CAPTCHAs.[39]

Human labor

It is possible to subvert CAPTCHAs by relaying them to a sweatshop of human operators who are employed to decode CAPTCHAs. A 2005 paper from a W3C working group said that they could verify hundreds per hour.[26] In 2010, the University of California at San Diego conducted a large scale study of CAPTCHA farms. The retail price for solving one million CAPTCHAs was as low as $1,000.[40]

Another technique consists of using a script to re-post the target site's CAPTCHA as a CAPTCHA to the attacker's site, which unsuspecting humans visit and solve within a short while for the script to use.[41] [42]

In 2023, the generative AI chatbot ChatGPT, tricked a TaskRabbit worker to solve a CAPTCHA by telling the worker it was not a robot and had impaired vision.[43]

Outsourcing to paid services

There are multiple Internet companies like *2Captcha* and *DeathByCaptcha* that offer human and machine backed CAPTCHA solving services for as low as US$0.50 per 1000 solved CAPTCHAs.[44] These services offer APIs and libraries that enable users to integrate CAPTCHA circumvention into the tools that CAPTCHAs were designed to block in the first place.[45]

Insecure implementation

Howard Yeend has identified two implementation issues with poorly designed CAPTCHA systems:[46] reusing the session ID of a known CAPTCHA image, and CAPTCHAs residing on shared servers.

Sometimes, if part of the software generating the CAPTCHA is client-side (the validation is done on a server but the text that the user is required to identify is rendered on the client side), then users can modify the client to display the un-rendered text. Some CAPTCHA systems use MD5 hashes stored client-side, which may leave the CAPTCHA vulnerable to a brute-force attack.[47]

Alternative CAPTCHAs

Some researchers have proposed alternatives including image recognition CAPTCHAs which require users to identify simple objects in the images presented. The argument in favor of these schemes is that tasks like object recognition are more complex to perform than text recognition and therefore should be more resilient to machine learning based attacks.

Chew et al. published their work in the 7th International Information Security Conference, ISC'04, proposing three different versions of image recognition CAPTCHAs, and validating the proposal with user studies. It is suggested that one of the versions, the anomaly CAPTCHA, is best with 100% of human users being able to pass an anomaly CAPTCHA with at least 90% probability in 42 seconds.[48] Datta et al. published their paper in the ACM Multimedia '05 Conference, named IMAGINATION (IMAge Generation for INternet AuthenticaTION), proposing a systematic way to image recognition CAPTCHAs. Images are distorted so image recognition approaches cannot recognise them.[49]

Microsoft (Jeremy Elson, John R. Douceur, Jon Howell, and Jared Saul) claim to have developed Animal Species Image Recognition for Restricting Access (ASIRRA) which ask users to distinguish cats from dogs. Microsoft had a beta version of this for websites to use.[50] They claim "Asirra is easy for users; it can be solved by humans 99.6% of the time in under 30 seconds. Anecdotally, users seemed to find the experience of using Asirra much more enjoyable than a text-based CAPTCHA." This solution was described in a 2007 paper to Proceedings of 14th ACM Conference on Computer and Communications Security (CCS).[51] It was closed in October 2014.[52]