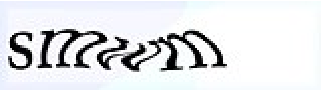
WIKIPEDIA

CAPTCHA

A **CAPTCHA** (/kæp.tʃə/, a contrived acronym for "Completely Automated Public Turing test to tell Computers and Humans Apart") is a type of challenge–response test used in computing to determine whether the user is human.[1]



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

The term was coined in 2003 by Luis von Ahn, Manuel Blum, Nicholas J. Hopper, and John Langford.[2] The most common type of CAPTCHA (displayed as Version 1.0) was first invented in 1997 by two groups working in parallel. This form of CAPTCHA requires someone to correctly evaluate and enter a sequence of letters or numbers perceptible in a distorted image displayed on their screen. Because the test is administered by a computer, in contrast to the standard Turing test that is administered by a human, a CAPTCHA is sometimes described as a reverse Turing test.[3]

This user identification procedure has received many criticisms, especially from people with disabilities, but also from other people who feel that their everyday work is slowed down by distorted words that are difficult to read. It takes the average person approximately 10 seconds to solve a typical CAPTCHA.[4]

History

Since the early days of the Internet, users have wanted to make text illegible to computers.[5] 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`, as well as numerous other variants, such that a filter could not possibly detect *all* of them. This later became known as leetspeak.[6]

One of the earliest commercial uses of CAPTCHAs was in the **Gausebeck–Levchin test**. In 2000, idrive.com began to protect its signup page[7] with a CAPTCHA and prepared to file a patent[5] on this seemingly novel technique. 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."[8] PayPal cofounder and CTO Max Levchin helped commercialize this early use.

A popular deployment of CAPTCHA technology, reCAPTCHA, was acquired by Google in 2009.[9] 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.[10]

Inventorship claims

Two teams have claimed to be the first to invent the CAPTCHAs used widely on the web today. The first team with Mark D. Lillibridge, Martín Abadi, Krishna Bharat, and Andrei Broder, used CAPTCHAs in 1997 at AltaVista to prevent bots from adding Uniform Resource Locator (URLs) to their web search engine. Looking for a way to make their images resistant to optical character recognition (OCR) attack, the team looked at the manual of their Brother scanner, which had recommendations for improving OCR's results (similar typefaces, plain backgrounds, etc.). The team created puzzles by attempting to simulate what the manual claimed would cause bad OCR.[11][12][13]

The second team to claim to be the first to invent CAPTCHAs with Luis von Ahn, Manuel Blum, Nicholas J. Hopper, and John Langford, first described CAPTCHAs in a 2003 publication[2] and subsequently received much coverage in the popular press. Their notion of CAPTCHA covers any program that can distinguish humans from computers.

The controversy of inventorship has been resolved by the existence of a 1997 priority date patent application by Eran Reshef, Gili Raanan and Eilon Solan (second group)[14] who worked at Sanctum on Application Security Firewall. 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". Lillibridge, Abadi, Bharat, and Broder (first group) published their patent in 1998.[15] Both patents predate other publications by several years, though they do not use the term CAPTCHA, they describe the ideas in detail and precisely depict the graphical CAPTCHAs used in the Web today.[16]

Characteristics

CAPTCHAs are, by definition, fully automated, requiring little human maintenance or intervention to administer, producing benefits in cost and reliability.

The algorithm used to create the CAPTCHA must be made public, though it may be covered by a patent. This is done to demonstrate that breaking it requires the solution to a difficult problem in the field of artificial intelligence (AI) rather than just the discovery of the (secret) algorithm, which could be obtained through reverse engineering or other means.[16]

Modern text-based CAPTCHAs are designed such that they require the simultaneous use of three separate abilities—invariant recognition, segmentation, and parsing—to correctly complete the task with any consistency.[17]

- Invariant recognition refers to the ability to recognize the large amount of variation in the shapes of letters. There is an overwhelmingly large number of versions of each character that a human brain can successfully identify. The same is not true for a computer, and teaching it to recognize all those differing formations is a challenging task.
- Segmentation, or the ability to separate one letter from another, is also made difficult in CAPTCHAs, as characters are crowded together with no white space in between.
- Context is also critical. The CAPTCHA must be understood holistically to correctly identify each character. For example, in one segment of a CAPTCHA, a letter might look like an "m". Only when the whole word is taken into context does it become clear that it is a *u* and an *n*.

Each of these problems poses a significant challenge for a computer, even in isolation. The presence of all three at the same time is what makes CAPTCHAs difficult to solve.[18]

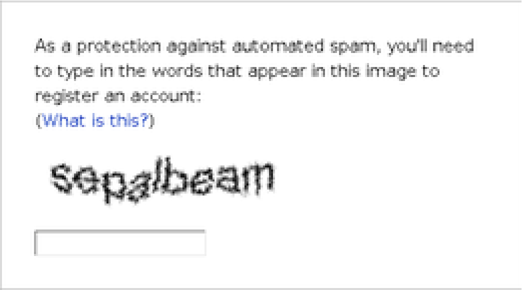
Unlike computers, humans excel at this type of task. While segmentation and recognition are two separate processes necessary for understanding an image for a computer, they are part of the same process for a person. For example, when an individual understands that the first letter of a CAPTCHA is an *a*, that individual also understands where the contours of that *a* are, and also where it melds with the contours of the next letter. Additionally, the human brain is capable of dynamic thinking based upon context. It is able to keep multiple explanations alive and then pick the one that is the best explanation for the whole input based upon contextual clues. This also means it will not be fooled by variations in letters.

Relation to AI

While used mostly for security reasons, CAPTCHAs also serve as a benchmark task for artificial intelligence technologies. According to an article by Ahn, Blum and Langford,[19] "any program that passes the tests generated by a CAPTCHA can be used to solve a hard unsolved AI problem."[20]

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. In the case of image and text based CAPTCHAs, if an AI were capable of accurately completing the task without exploiting flaws in a particular CAPTCHA design, then it would have solved the problem of developing an AI that is capable of complex object recognition in scenes.[19]

Accessibility



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.

CAPTCHAs based on reading text — or other visual-perception tasks — prevent blind or visually impaired users from accessing the protected resource.[21] However, CAPTCHAs do not have to be visual. Any hard artificial intelligence problem, such as speech recognition, can be used as the basis of a CAPTCHA. Some implementations of CAPTCHAs permit users to opt for an audio CAPTCHA, though a 2011 paper demonstrated a technique for defeating the popular schemes at the time.[22]

For non-sighted users (for example blind users, or color blind people on a color-using test), visual CAPTCHAs present serious problems.[23] 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 completely 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. In other cases, those with sight difficulties can choose to identify a word being read to them.

While providing an audio CAPTCHA allows blind users to read the text, it still hinders those who are both blind and deaf. According to sense.org.uk, about 4% of people over 60 in the UK have both vision and hearing impairments. There are about 23,000 people in the UK who have serious vision and hearing impairments. According to The National Technical Assistance Consortium for Children and Young Adults Who Are Deaf-Blind (NTAC), the number of deafblind children in the USA increased from 9,516 to 10,471 during the period 2004 to 2012.[24] Gallaudet University quotes 1980 to 2007 estimates which suggest upwards of 35,000 fully deafblind adults in the USA.[25] Deafblind population estimates depend heavily on the degree of impairment used in the definition.

The use of CAPTCHA thus excludes a small number of individuals from using significant subsets of such common Web-based services as PayPal, Gmail, Orkut, Yahoo!, many forum and weblog systems, etc.[26]

Even for perfectly sighted individuals, new generations of graphical CAPTCHAs, designed to overcome sophisticated recognition software, can be very hard or impossible to read.

A method of improving CAPTCHA to ease the work with it was proposed by ProtectWebForm and named "Smart CAPTCHA".[27] 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.

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.

Other kinds of challenges, such as those that require understanding the meaning of some text (e.g., a logic puzzle, trivia question, or instructions on how to create a password) can also be used as a CAPTCHA. Again, there is little research into their resistance against countermeasures.

Circumvention

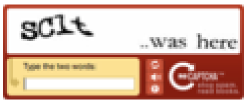
There are a few approaches to defeating CAPTCHAs: using cheap human labor to recognize them, exploiting bugs in the implementation that allow the attacker to completely bypass the CAPTCHA, and finally using machine learning to build an automated solver.[28] According to former Google "click fraud czar" Shuman Ghosemajumder, there are numerous services which solve CAPTCHAs automatically.[29]

Machine learning-based attacks

In its earliest iterations there was not a systematic methodology for designing or evaluating CAPTCHAs.[18] 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 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. These methods proved brittle however, and slight changes to the CAPTCHA were easily able to thwart them. Modern CAPTCHAs like reCAPTCHA no longer rely just on fixed patterns but instead present variations of characters that are often collapsed together, making segmentation almost impossible. These newest iterations have been much more successful at warding off automated tasks.[30]

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.



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 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%.[31] However, Luis von Ahn, a pioneer of early CAPTCHA and founder of reCAPTCHA, expressed skepticism, stating: "It's hard for me to be impressed since I see these every few months." He pointed out that 50 similar claims to that of Vicarious had been made since 2003.[32]

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. They concluded that text distortion based CAPTCHAs schemes should be considered insecure moving forward.[30]

In October 2018 at ACM CCS'18 conference, Ye et al. presented a deep learning-based attack that could successfully solve all 11 text captcha schemes used by the top-50 popular website in 2018 with a high success rate. Their work shows that an effective CAPTCHA solver can be trained using as few as 500 real CAPTCHAs, showing that it is possible to quickly launch an attack of a new text CAPTCHA scheme.[33]

Cheap or unwitting 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 stated that such an operator could verify hundreds per hour.[21] In 2010, the University of California at San Diego conducted a large scale study of CAPTCHA farms and found out that the retail price for solving one million CAPTCHAs was as low as $1,000.[34]

Another technique that has been described consists of using a script to re-post the target site's CAPTCHA as a CAPTCHA to a site owned by the attacker, which unsuspecting humans visit and correctly solve within a short while for the script to use.[35] This technique is likely to be economically unfeasible for most attackers due to the cost of attracting enough users and running a popular site.[36]

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.[37] 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.

Insecure implementation

Howard Yeend has identified two implementation issues with poorly designed CAPTCHA systems:[38]

- Some CAPTCHA protection systems can be bypassed without using OCR simply by reusing the session ID of a known CAPTCHA image
- CAPTCHAs residing on shared servers also present a problem; a security issue on another virtual host may leave the CAPTCHA issuer's site vulnerable

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.

Notable attacks

Some notable attacks against various CAPTCHAs schemas include:

- Mori et al. published a paper in IEEE CVPR'03 detailing a method for defeating one of the most popular CAPTCHAs, EZ-Gimpy, which was tested as being 92% accurate in defeating it.[39] The same method was also shown to defeat the more complex and less-widely deployed Gimpy program 33% of the time. However, the existence of implementations of their algorithm in actual use is indeterminate at this time.
- PWNtcha has made significant progress in defeating commonly used CAPTCHAs, which has contributed to a general migration towards more sophisticated CAPTCHAs.[40]
- Podec, a trojan discovered by the security company Kaspersky, forwards CAPTCHA requests to an online human translation service that converts the image to text, fooling the system. Podec targets Android mobile devices.[41]

Alternative CAPTCHAs schemas

With the demonstration that text distortion based CAPTCHAs are vulnerable to machine learning based attacks, 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 typically more complex to perform than text recognition and therefore should be more resilient to machine learning based attacks. Here are some of notable alternative CAPTCHA schemas:

- 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.[42]
- 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 in such a way that state-of-the-art image recognition approaches (which are potential attack technologies) fail to recognize them.[43]
- 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.[44] 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).[45] However, this project was closed in October 2014 and is no longer available.[46]

See also

- Defense strategy (computing)
- NuCaptcha
- Proof-of-work system
- reCAPTCHA

References

1. "The reCAPTCHA Project – Carnegie Mellon University CyLab" (https://web.archive.org/web/20171027203659/https://www.cylab.cmu.edu/partners/success-stories/recaptcha.html) . www.cylab.cmu.edu. Archived from the original (https://www.cylab.cmu.edu/partners/success-stories/recaptcha.html) on 2017-10-27. Retrieved 2017-01-13.

2. von Ahn, Luis; Blum, Manuel; Hopper, Nicholas J.; Langford, John (May 2003). CAPTCHA: Using Hard AI Problems for Security (https://link.springer.com/content/pdf/10.1007/3-540-39200-9_18.pdf) (PDF). EUROCRYPT 2003: International Conference on the Theory and Applications of Cryptographic Techniques. doi:10.1007/3-540-39200-9_18 (https://doi.org/10.1007%2F3-540-39200-9_18) .

3. Mayumi Takaya; Yusuke Tsuruta2; Akihiro Yamamura1. "Reverse Turing Test using Touchscreens and CAPTCHA⚹" (http://isyou.info/jowua/papers/jowua-v4n3-3.pdf) (PDF). Akita University.

4. Bursztein, Elie; Bethard, Steven; Fabry, Celine; Mitchell, John C.; Jurafsky, Dan (2010). "How Good are Humans at Solving CAPTCHAs? A Large Scale Evaluation" (https://web.stanford.edu/~jurafsky/burszstein_2010_captcha.pdf) (PDF). Proceedings of the 2010 IEEE Symposium on Security and Privacy: 399–413. CiteSeerX 10.1.1.164.7848 (https://citeseerx.ist.psu.edu/viewdoc/summary?doi=10.1.1.164.7848) . doi:10.1109/SP.2010.31 (https://doi.org/10.1109%2FSP.2010.31) . ISBN 978-1-4244-6894-2. S2CID 14204454 (https://api.semanticscholar.org/CorpusID:14204454) . Retrieved March 30, 2018.

5. "idrive turing patent application" (https://drive.google.com/open?id=0BzbOLm20p6CrOS1mWEhITGJ4d2s) . Retrieved 2017-05-19.

6. "h2g2 – An Explanation of l33t Speak – Edited Entry" (http://www.bbc.co.uk/dna/h2g2/A787917) . h2g2. Retrieved 2015-06-03.

7. "idrive turing signup page" (https://drive.google.com/open?id=0BzbOLm20p6CrUE1SSXp5Zjl2MW8) . Google Drive. Retrieved 2017-05-19.

8. Stringham, Edward P (2015). Private Governance : creating order in economic and social life. Oxford University Press. p. 105. ISBN 978-0-19-936516-6. OCLC 5881934034 (https://www.worldcat.org/oclc/5881934034) .

9. "Teaching computers to read: Google acquires reCAPTCHA" (https://googleblog.blogspot.com/2009/09/teaching-computers-to-read-google.html) . Google Official Blog.

10. Gugliotta, Guy (28 March 2011). "Deciphering Old Texts, One Woozy, Curvy Word at a Time" (https://www.nytimes.com/2011/03/29/science/29recaptcha.html) . The New York Times.

11. Feng, Yunhe; Cao, Qing; Qi, Hairong; Ruoti, Scott (June 2020). "SenCAPTCHA: A Mobile-First CAPTCHA Using Orientation Sensors" (https://www.researchgate.net/publication/341459932) . doi:10.1145/3397312 (https://doi.org/10.1145%2F3397312) .

12. Soto, Micah (24 May 2019). "The origin of CAPTCHA and reCAPTCHA" (https://tipsmake.com/the-origin-of-captcha-and-recaptcha) .

13. United States US6195698B1 (https://patents.google.com/patent/US6195698B1/en) , Mark D. Lillibridge; Krishna Bharat & Martin Abadi et al., published 1998-04-13

14. US 2005/0114705 A1 (https://patentimages.storage.googleapis.com/9c/fc/21/1188d59d94d268/US20050114705A1.pdf) , Reshef, Eran; Raanan, Gil & Solan, Eilon, "Method and system for discriminating a human action from a computerized action", published 26 May 2005

15. U.S. Patent 6,195,698. Method for selectively restricting access to computer systems. Filed on April 13, 1998 and granted on February 27, 2001. Available at google.com (http://www.google.com/patents/US6195698)

16. Justie, Brian (2020). "Little history of CAPTCHA". Internet Histories. **5**: 30–47. doi:10.1080/24701475.2020.1831197 (https://doi.org/10.1080%2F24701475.2020.1831197) . S2CID 228834122 (https://api.semanticscholar.org/CorpusID:228834122) .

17. Chellapilla, Kumar; Larson, Kevin; Simard, Patrice; Czerwinski, Mary. "Designing Human Friendly Human Interaction Proofs (HIPs)" (https://web.archive.org/web/20150410195118/http://research.microsoft.com/pubs/101726/HIPSCHI2005.pdf) (PDF). Microsoft Research. Archived from the original (https://research.microsoft.com/pubs/101726/HIPSCHI2005.pdf) (PDF) on 10 April 2015.

18. Bursztein, Elie; Martin, Matthieu; Mitchell, John C. (2011). "Text-based CAPTCHA Strengths and Weaknesses" (https://www.elie.net/publication/text-based-captcha-strengths-and-weaknesses) . ACM Computer and Communication Security 2011 (CSS'2011).

19. von Ahn, Luis; Blum, Manuel; Hopper, Nicholas J.; Langford, John (2003). "CAPTCHA: Using Hard AI Problems for Security" (https://link.springer.com/content/pdf/10.1007/3-540-39200-9_18.pdf) (PDF). Advances in Cryptology — EUROCRYPT 2003. Lecture Notes in Computer Science. Vol. 2656. pp. 294–311. doi:10.1007/3-540-39200-9_18 (https://doi.org/10.1007%2F3-540-39200-9_18) . ISBN 978-3-540-14039-9.

20. Moy G, N Jones and C Harkless (2004) "Distortion estimation techniques in solving visual CAPTCHAs (http://www.cs.duke.edu/courses/cps296.3/spring07/breaking_captchas.pdf) ", Proceedings of the 2004 IEEE Computer Society Conference on Computer Vision and Pattern Recognition.

21. May, Matt (2005-11-23). "Inaccessibility of CAPTCHA" (http://www.w3.org/TR/turingtest/) . W3C. Retrieved 2015-04-27.

22. Bursztein, Elie; Beauxis, Romain; Perito, Hristo; Paskov, Daniele; fabry, Celine; Mitchell, John C. (2011). "The failure of noise-based non-continuous audio captchas" (https://www.elie.net/publication/the-failure-of-noise-based-non-continuous-audio-captchas) . IEEE Symposium on Security and Privacy (S&P), 2011: 19–31. doi:10.1109/SP.2011.14 (https://doi.org/10.1109%2FSP.2011.14) . ISBN 978-1-4577-0147-4. S2CID 6933726 (https://api.semanticscholar.org/CorpusID:6933726) .

23. Shea, Michael (19 November 2015). "CAPTCHA: Spambots, eBooks and the Turing Test" (http://www.theskinny.co.uk/tech/features/captcha-spambots-ebooks-and-the-turing-test) . The Skinny. Retrieved 9 January 2016.

24. "National Child Count Annual Reports" (http://nationaldb.org/library/page/2199) . TA&D Network. National Consortium on Deaf-Blindness. November 30, 2012. Retrieved 27 November 2013.

25. Harrington, Tom; Rutherford, Jane. "American deaf-blind population" (http://libguides.gallaudet.edu/content.php?pid=119476&sid=1029203) . Deaf Statistics. Gallaudet University Library. Retrieved 27 November 2013.

26. "Inaccessibility of CAPTCHA" (https://www.w3.org/TR/2019/NOTE-turingtest-20191209/Overview.html) . www.w3.org. Retrieved 2020-10-31.

27. "Smart Captcha" (https://web.archive.org/web/20161104163541/http://protectwebform.com/smartcaptcha) . Protect Web Form .COM. 2006-10-08. Archived from the original (http://www.protectwebform.com/smartcaptcha) on 2016-11-04. Retrieved 2017-09-15.

28. Jakobsson, Markus (August 2012). The death of the Internet (http://eu.wiley.com/WileyCDA/WileyTitle/productCd-1118062418.html) . Retrieved 4 April 2016.

29. Ghosemajumder, Shuman (8 December 2015). "The Imitation Game: The New Frontline of Security" (http://www.infoq.com/presentations/ai-security) . InfoQ. InfoQ. Retrieved 8 December 2015.

30. Bursztein, Elie; Aigrain, Johnathan; Mosciki, Angelika; Michell, John C. (August 2014). The End is Nigh: Generic Solving of Text-based CAPTCHAs (https://www.elie.net/publication/the-end-is-nigh-generic-solving-of-text-based-captchas) . WoOT 2014: Usenix Workshop on Offensive Security.

31. Summers, Nick. "Vicarious claims its AI software can crack up to 90% of CAPTCHAs offered by Google, Yahoo and PayPal" (https://thenextweb.com/insider/2013/10/28/vicarious-claims-ai-software-can-now-crack-90-captchas-google-yahoo-paypal/) . TNW.

32. Hof, Robert. "AI Startup Vicarious Claims Milestone In Quest To Build A Brain: Cracking CAPTCHA" (https://www.forbes.com/sites/roberthof/2013/10/28/ai-startup-vicarious-claims-milestone-in-quest-to-build-a-brain-craking-captcha/) . Forbes.

33. "Yet Another Text Captcha Solver: A Generative Adversarial Network Based Approach" (https://eprints.lancs.ac.uk/id/eprint/126984/1/ccs18.pdf) (PDF). 25th ACM Conference on Computer and Communications Security (CCS), 2018. doi:10.1145/3243734.3243754 (https://doi.org/10.1145%2F3243734.3243754) . S2CID 53106794 (https://api.semanticscholar.org/CorpusID:53106794) .

34. Motoyama, Marti; Levchenko, Kirill; Kanich, Chris; McCoy, Damon; Geoffrey, Voelker; Savage, Stefan (August 2010). Re: CAPTCHAs-Understanding CAPTCHA-Solving Services in an Economic Context.s (http://static.usenix.org/event/sec10/tech/full_papers/Motoyama.pdf) (PDF). USENIX Security Symposium, 2010.

35. Doctorow, Cory (2004-01-27). "Solving and creating captchas with free porn" (https://web.archive.org/web/20060209040456/http://www.boingboing.net/2004/01/27/solving_and_creating.html) . Boing Boing. Archived from the original (https://www.boingboing.net/2004/01/27/solving_and_creating.html) on 2006-02-09. Retrieved 2015-04-27.

36. "Hire People To Solve CAPTCHA Challenges" (http://petmail.lothar.com/design.html#auto35) . Petmail Design. 2005-07-21. Retrieved 2015-04-27.

37. "Top 10 Captcha Solving Services Compared" (http://www.prowebscraper.com/blog/top-10-captcha-solving-services-compared/) . Retrieved 2018-12-10.

38. Yeend, Howard (2005). "Breaking CAPTCHAs Without Using OCR" (https://web.archive.org/web/20170625165854/http://www.puremango.co.uk/2005/11/breaking_captcha_115/) . (pureMango.co.uk). Archived from the original (http://www.puremango.co.uk/cm_breaking_captcha_115.php) on 2017-06-25. Retrieved 2006-08-22.

39. "Breaking a Visual CAPTCHA" (https://web.archive.org/web/20050403213029/http://www.cs.berkeley.edu/~mori/gimpy/mori_gimpy.pdf) (PDF). Cs.berkeley.edu. 2002-12-10. Archived from the original (http://www.cs.berkeley.edu/~mori/gimpy/mori_gimpy.pdf) (PDF) on 2005-04-03. Retrieved 2017-09-15.

40. "PWNtcha – Caca Labs" (http://sam.zoy.org/pwntcha/) . Sam.zoy.org. 2009-12-04. Retrieved 2013-09-28.

41. "Kaspersky discovers CAPTCHA-duping Podec malware" (https://www.scmagazineuk.com/kaspersky-discovers-captcha-duping-podec-malware/article/1478464) . SC Magazine UK. 2015-03-11. Retrieved 2016-11-18.

42. "Image Recognition CAPTCHAs" (https://web.archive.org/web/20130510022240/http://www.cs.berkeley.edu/~tygar/papers/Image_Recognition_CAPTCHAs/imagecaptcha.pdf) (PDF). Cs.berkeley.edu. Archived from the original (http://www.cs.berkeley.edu/~tygar/papers/Image_Recognition_CAPTCHAs/imagecaptcha.pdf) (PDF) on 2013-05-10. Retrieved 2013-09-28.

43. "Imagination Paper" (http://infolab.stanford.edu/~wangz/project/imsearch/IMAGINATION/ACM05/) . Infolab.stanford.edu. Retrieved 2013-09-28.

44. "Asirra is a human interactive proof that asks users to identify photos of cats and dogs" (https://web.archive.org/web/20081215032402/http://research.microsoft.com/en-us/um/redmond/projects/asirra/) . Microsoft. Archived from the original (https://www.microsoft.com/en-us/research/publication/asirra-a-captcha-that-exploits-interest-aligned-manual-image-categorization/) on 15 December 2008.

45. "Asirra: A CAPTCHA that Exploits Interest-Aligned Manual Image Categorization" (https://www.microsoft.com/en-us/research/publication/asirra-a-captcha-that-exploits-interest-aligned-manual-image-categorization/) . Microsoft.

46. "Microsoft's Asirra project closed" (https://web.archive.org/web/20090112032323/http://research.microsoft.com/en-us/um/redmond/projects/asirra/installation.aspx) . Archived from the original (http://research.microsoft.com/en-us/um/redmond/projects/asirra/installation.aspx) on 12 January 2009.

Further references

- von Ahn, L; M. Blum and J. Langford. (2004) "Telling humans and computers apart (automatically) (http://www.cs.cmu.edu/afs/cs/Web/People/aladdin/papers/pdfs/y2004/captcha_cacm.pdf) ". *Communications of the ACM*, **47**(2):57–60.

External links

CAPTCHA
at Wikipedia's sister projects

Definitions from Wiktionary

Media from Commons

Textbooks from Wikibooks

Data from Wikidata

Documentation from MediaWiki

- CAPTCHA (https://curlie.org/Computers/Internet/Abuse/CAPTCHA/) at Curlie
- Verification of a human in the loop, or Identification via the Turing Test (http://www.wisdom.weizmann.ac.il/~naor/PAPERS/human_abs.html) , Moni Naor, 1996.
- Inaccessibility of CAPTCHA: Alternatives to Visual Turing Tests on the Web (http://www.w3.org/TR/turingtest/) , a W3C Working Group Note.
- CAPTCHA History (https://web.archive.org/web/20120205201803/http://www2.parc.com/istl/projects/captcha/history.htm) from PARC.
- Reverse Engineering CAPTCHAs (https://web.archive.org/web/20170915204258/https://pdfs.semanticscholar.org/692a/31f65e29ea3667de46933245f53bda55a65b.pdf) Abram Hindle, Michael W. Godfrey, Richard C. Holt, 2009-08-24