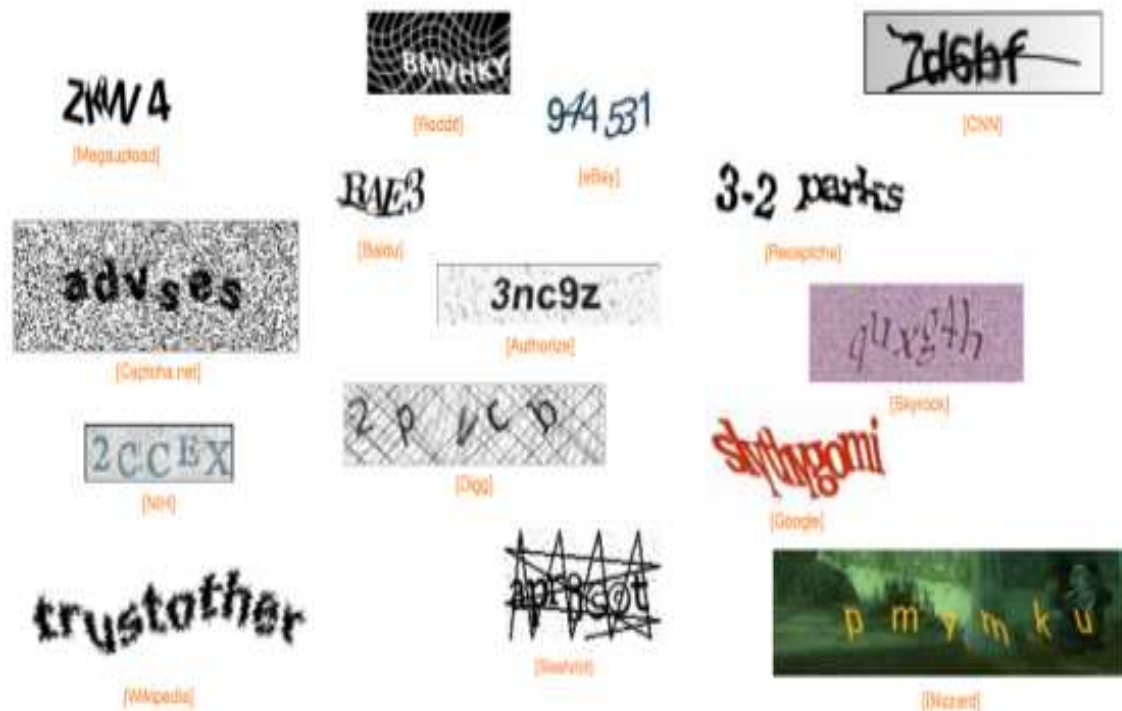


The word, "Captcha" stands for **Completely Automated Public Turing test to tell Computers and Humans Apart**. You may have seen Captchas, as shown below. Many Web sites force you to use these often unreadable and always annoying distorted letters to prove that you're really a human.



Examples of popular Captchas. (Credit: [Stanford University](#))

A team of Stanford University researchers has found that many Captchas don't work well at all. The team has invented a standard way to decode those irksome letters and numbers found in Captchas on many major Web sites, including Visa's Authorize.net, Blizzard, eBay, and Wikipedia. Their decoding technique borrows concepts from the field of machine vision, which has developed techniques to control robots by removing noise from images and detecting shapes.

The Stanford tool, called Decaptcha, uses these algorithms to clean up the image so it can be split into more readily recognized letters and numbers. "Most Captchas are designed without proper testing and no usability testing," said Elie Bursztein, 31, a postdoctoral researcher at the Stanford Security Laboratory. "We hope our work will push people to be more rigorous in their approach in Captcha design."

Scheme	Recall	Precision	Anti-segmentation
Authorize	84%	66%	background confusion
Baidu	98%	5%	collapsing
Blizzard	75%	70%	background confusion
Captcha.net	96%	73%	background confusion
CNN	50%	16%	line
Digg	86%	20%	line
eBay	95%	43%	collapsing
Google	0%	0%	collapsing
Megaupload	n/a	93%	collapsing
NIH	87%	72%	background confusion
Recaptcha	0%	0%	collapsing
Reddit	71%	42%	background confusion
Skyrock	30%	2%	background confusion
Slashdot	52%	35%	lines
Wikipedia	57%	25%	n/a

This chart, from the Stanford research team shows how successful Decaptcha was in decoding each Web site's Captchas. The column labeled "precision" shows the success rate.

Decaptcha was able to decode 66 percent of the Captchas used by Visa's Authorize.net payment site, 70 percent of Blizzard Entertainment's Captchas -- the company's games include World of Warcraft and Diablo -- and 25 percent of Wikipedia's. About one-fifth of Digg.com's Captchas and almost that many of CNN.com's were decodable. An important statistic from the Stanford team is that any decoding rate over 1 percent means that particular Captcha is too broken to continue to use.

Blizzard uses more than just Captchas to secure their systems. A Blizzard representative, Shon Damron, in an October, 2011, interview with CNET, also noted that it is common knowledge that Captchas are fundamentally unable to fully guarantee application security, but they do protect against certain threats. Shon also said that while Blizzard uses Captchas as an initial layer of security, primarily to minimize spam with regard to new account creation. Shon also noted that Captchas represent one of many different security technologies Blizzard employs to protect our infrastructure and customers.

The security of Captchas is important because they're used to defend against malicious 'bots, including operators of botnets who try to automatically create accounts on Web e-mail services to send spam. Captchas are also used to curb bot-generated comments and automated ballot-stuffing in online polls.

The only tested Captchas that withstood the Stanford researchers' attacks were Google's The researchers ran into a remarkable zero percent success rate when trying to decode Google's slanted-red-letters Captcha, used in Gmail, and the fuzzy-lettered ReCaptcha, which was created at Carnegie Mellon University and acquired by Google in 2009. A research group from Newcastle University in the UK has reported finding better success against Google's Captchas.

According to Google's estimates, ReCaptcha, which is free, is used over 100,000 Web sites including Twitter, Facebook, Craigslist, Ticketmaster, and Microsoft. The Stanford research team did not test Yahoo, Amazon, and LinkedIn's Captchas because it was too difficult to get them to appear consistently.

Bursztein hopes to encourage Web developers to think about Captchas more systematically -- as a computer science challenge, not just a simple security problem that can be solved without adequate testing. He noted that you should not "roll your own Captchas unless you know what you are doing" and likens current Captcha efforts to encryption research in the 1980s, when developers tried to invent their own algorithms. Over time, researchers realized that peer review and a security analysis by someone trying to break the code was necessary.

The Stanford researchers say they have no plans to release Decaptcha. "We don't want bad guys to use it against companies," Bursztein says.

"Decaptcha is not meant to be released to the general public. We do provide it to companies that wish to test their Captchas. Our goal is to make the Web a better place, not to harm users."