

# Rage against the machines: A computer engineer battles malicious bots

April 6 2015

---



Credit: George Hodan/Public Domain

Defending websites from malicious intruder bots is not unlike fighting viruses: neutralize them and they reinvent themselves, finding new ways to penetrate. But IT security designers still hold an advantage over some automated programs masquerading as people. To date, there are human abilities too complex to imitate.

Exploiting that weakness is central to an Internet security [technology](#) developed by Nirwan Ansari, Distinguished Professor of Electrical and Computer Engineering, and two of his former students, who have come up with a new method for distinguishing humans from computers. Their next-gen CAPTCHA - a brief test that computer users must pass in order to access a website - requires viewers to identify text, but presents it in video animation rather than in the distorted, static letters users now identify and reproduce to gain admittance.

Recently patented, their "Simultaneous Contrast and the Persistence of Vision CAPTCHA" relies on the human capacity to process rapidly displayed, discrete images as continuous animation. Moviegoers, for example, are able to read frames passing by at the rate of 24 per second as a coherent narrative because a visual imprint of the passing frame remains briefly in the brain, allowing it to segue seamlessly to the next. The technology also depends on the eye's tendency to interpret colors differently if they are set against a contrasting background, adding an extra hurdle for computers.

"Current static CAPTCHAs can be easily breached now and so the idea was to make the test more robust. Machines do not have our eyes - our complex visual intelligence - and we exploit that advantage," Ansari explains. "In our video-based CAPTCHA, if you capture one frame, it tells you nothing. If you combine the frames, together they still tell you nothing. We're relying on a unique human ability to connect images. We display them against a contrasting color to make them even more difficult for bots to interpret. So it is easy for humans to pass the test by simply identifying the text of the short video, but difficult for machines to extract meaning from it."

He says the new test was also designed to simplify access - for people.

"In order to defeat sophisticated attackers who keep improvising their

breaking techniques, CAPTCHAs are becoming tougher for humans to solve. We keep our text simple and thus easy to recognize," Ansari adds, noting that the system was devised for use as a safeguard against directory attacks and website intrusions, among other vulnerable access points and transactions.

Two of his former students, Amey Shevtekar, a computer engineering graduate student who has since earned his Ph.D., and Christopher Neylan, an undergraduate from The College of New Jersey working with him under a Research Experiences for Undergraduates (REU) grant from the National Science Foundation, helped him design the test and are named on the patent (8925057).

CAPTCHA, an acronym for Completely Automated Public Turing-test to tell Computers and Humans Apart, refers to a challenge conceived by Alan Turing, the British mathematician, computing pioneer and cryptanalyst, of a machine's ability to successfully imitate human responses. Turing's central role in cracking the Nazi's Enigma Code during World War II was recently dramatized in the film, *The Imitation Game*.

Ansari's CAPTCHA technology earned him his 25th patent since 2000, the year he received his first for an algorithm to control congestion on ATM (Asynchronous Transfer Mode) cell relay switches, alleviating gridlock in a fair, fast manner. Along the way, he has also received patents for methods to trace cyber attacks, and to detect and mitigate [denial-of-service attacks](#), automated assaults that shut down a website by flooding it with traffic.

Over the past few years, Ansari has become a noted expert in "green communications," whose aim is to transform the country's communications infrastructure into a reliable, energy-efficient one. What links his research, beginning with his 1988 Ph.D. dissertation on

programs that enable computers to recognize patterns and objects, is computational intelligence.

"Ironically, advances in networking technologies are furthering the rapid propagation of worms and the growth of botnets, thus exacerbating threats to the integrity of the Internet," he notes. "Meanwhile, bots themselves have become increasingly sophisticated since the early days of denial-of-service attacks. These days, attackers are professionals motivated by financial incentives and cyberterrorism, and they bring higher sophistication to attack techniques that can evade detection and the potential for drastic damage. There is never a perfect system and so we continue to play catch-up. There will always be two teams: cops and thieves."

Altogether, NJIT researchers currently hold 185 U.S. patents, with another 133 pending. Patents expire after 20 years.

Provided by New Jersey Institute of Technology

Citation: Rage against the machines: A computer engineer battles malicious bots (2015, April 6) retrieved 20 April 2024 from <https://phys.org/news/2015-04-rage-machines-malicious-bots.html>

This document is subject to copyright. Apart from any fair dealing for the purpose of private study or research, no part may be reproduced without the written permission. The content is provided for information purposes only.