Stanford University researchers break NuCaptcha video security

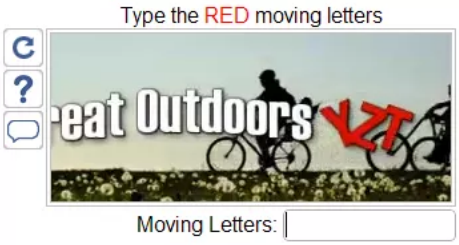
Borrowing from the field of machine vision, Stanford University researchers have discovered how to solve over 90 percent of NuCaptcha's are-you-a-human video challenges.

Security

by **Declan McCullagh**
February 17, 2012 1:51 PM PST
@declanm

When it launched in 2010, **NuCaptcha touted its proprietary technology** as being able to "provide the highest level of security available" by using video streams to display those distorted letters you type in to prove you're really a human.

Now, however, the company's claims of providing "the **next generation of Captcha security**" look a tad optimistic.



An example still image taken from a NuCaptcha video stream.

A team of Stanford University researchers said today that they discovered a way to break the security of a recent version of NuCaptcha's **video Captcha** by borrowing concepts from the field of machine vision, which developed techniques to control robots by removing noise from images and detecting shapes. NuCaptcha is a privately-funded startup with its headquarters in Vancouver, B.C.

"We are able to break NuCaptcha's video scheme with over 90 percent success," says **Elie Bursztein**, 31, who worked on the analysis as a postdoctoral researcher at the Stanford Security Laboratory before leaving at the end of December. Bursztein says he believes, however, that NuCaptcha's algorithm can be fixed using a technique he calls tracking resistance.

Any decoding rate over 1 percent, the Stanford team says, means that particular Captcha is too broken to continue to use. Other collaborators on the project include Matthieu Martin, Shang Ping, Jonathan Aigrain, Mike Bailey and computer science professor John Mitchell.

For its part, NuCaptcha told CNET in a statement: "No single Captcha will defend against every possible attack. Our strategy is to develop a collection of responses and, as appropriate, to deploy them to individual users instead of presenting a single rigid defense." The statement said this research suggested ways NuCaptcha could be improved, such as varying the length of the code string and where it appears in the video stream, and altering a letter's appearances in adjacent frames."

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.

By contrast, Google's image-based Captchas, which can be harder for a human to decipher, fared much better against attacks. The Stanford researchers ran into a **remarkable zero percent success rate** last fall, as CNET reported at the time, 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.

Elie Bursztein, who worked on the NuCaptcha analysis as a postdoctoral researcher at the Stanford Security Laboratory

Declan McCullagh/CNET

Bursztein, who will be speaking about Captchas and tracking resistance at the **RSA Conference** in San Francisco next month, says he hopes his work will encourage a broader dialogue in the computer science community about how to create a better video Captcha. (Captcha stands for Completely Automated Public Turing test to tell Computers and Humans Apart.)

Because of advances in computer vision -- namely, **optical flow algorithms** -- trying to prevent the computer from finding moving objects is a "lost cause," he says.

NuCaptcha says they have a "higher security" Captcha with more distortions that would be harder to break; Bursztein replies that his team mimicked the behavior of an automated bot, and after trying to attack the hardest NuCaptcha variant available, found "we were able to break the Captcha we downloaded." Even if the letters were more distorted, he says, that wouldn't provide an effective defense because it would not "impact an optical flow algorithm used to separate the letters."

NuCaptcha chief technologist **Christopher Bailey** told CNET this afternoon that in response to the Stanford research that he reviewed in advance a few weeks ago, the company has taken steps to "address that specific" attack.

Bailey said that NuCaptcha has chosen to enable "inter-frame warping" of characters in response to the paper. "Our practice is to identify potential weaknesses in our system, develop fixes for them, and then deploy those fixes as appropriate," he said. "Dr. Bursztein has developed a fascinating algorithm that takes advantage of that static feature, and so we deployed our fix." (Bursztein told CNET that he has not evaluated the effectiveness of the modified algorithm: "I don't want to make any guesses. I want to test.")

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 likens it to the state of 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.