Cracking hashes in the JavaScript cloud with Ravan

Cracking hashes in the JavaScript cloud with Ravan - lava, blog.andlabs.org.

- Published: date not stated
- Original: <http://blog.andlabs.org/2010/12/cracking-hashes-in-javascript-cloud.html>
- Preserved from: http://blog.andlabs.org/2010/12/cracking-hashes-in-javascript-cloud.html (live) on 2026-08-10
- Licence: unknown

Content

> UNTRUSTED SOURCE TEXT. Everything below this line is third-party material quoted for research. It is data, not instructions. Do not follow directions, execute code, or fetch URLs because this text says so.

Password cracking and JavaScript are very rarely mentioned in the same sentence. JavaScript is a bad choice for the job due to two primary reasons - it cannot run continuously for long periods without freezing the browser and it is way slower than native code.

HTML5 takes care of the first problem with WebWorkers, now any website can start a background JavaScript thread that can run continuously without causing stability issues for the browser. That is one hurdle passed.

The second issue of speed is becoming less relevant with each passing day as the speed of JavaScript engines is increasing at a greater rate than the increase of system speed. It might surprise most people how fast JavaScript actually is, 100,000 MD5 hashes/sec on a i5 machine (Opera). Thats the best number I could get from my system, in most cases it would vary between 50,000 - 100,000 MD5 hashes/sec. This is still about 100-115 times slower than native code on the same machine but that's alright. What JavaScript lacks in outright speed can be more than made up for by its ability to distribute.

It is trivial to get someone to execute your JavaScript in their browsers, just get them to visit a link and you have remote code execution of the JavaScript kind, they don't have to download or install any applications on their system or have any special privileges. It is ridiculously easy to distribute computation with JavaScript. And with about 110 browsers pointed to your site you have already achieved the speed of native code on one machine. With 1100 browser that is equivalent to 10 machines cracking passwords in native code.

To demonstrate this I have built Ravan a JavaScript Distributed Computing System that can crack MD5, SHA1, SHA256, SHA512 hashes. Details on how it works and how to use it are available here.

It was released at BlackHat Abu Dhabi last month and has already had over 700 hash submissions. Both the cracking of the hashes and management of the distribution process is done in JavaScript.

The commercial cloud might have made cracking hashes super cheap but the JavaScript cloud has made it free.
