Its Halloween for Passwords

David Holmes, 2010-01-11

8 is the new 7. No wait, its 14.

Way, way back in the day, you could **drag your knuckles around the internet with a 7-character** alphanumeric password as your basic defense. Over time, security-sensitive sites (Banks, et al) have begun requiring 8 characters, not just 7. Even **Comcast** requires 8 and as far as I can tell, the only assets they are protecting are your phone records and your email.

Complain all you want, but **the truth is that the bad guys have all the big guns now** with their million-PC zombie farms, and a 7 character password can be broken in microseconds. 8 characters is better, of course, so if you are one of those knuckle-draggers, maybe its time to design your next **DEFAULT** password; you know, the one that you use on every other site on the internet.

http://links.f5.com/bowFxJ - *Cryptographer creates a clearing house of 14 Million cracked passwords*

But wait, is 8 characters enough? **That depends on a couple of things**. If your password just one long word, or two simple words catted together (TwitterRocks), then that's probably not good enough. Here's a link to a cryptographer that's created a "*clearinghouse*" of 14 million passwords across the internet. You could download his TXTFILE and make sure that your new password isn't in there; that might be a good way to at least get some measure of uniqueness.

http://links.f5.com/dzR3Ox – *GPUs hacking passwords*

For years people have been talking about how to leverage the vast computing power represented by your typical modern GPU (Graphics Card). This idea has become theoretically more realizable now that there is an open SDK to nVideo's CUDA. Now imagine millions of zombie PCs each running hardware-accelerated password crackers. No, wait, don't imagine that, you might have nightmares.

http://links.f5.com/cn5kyM - *SDD as a technology for creating rainbow tables.*

Now here's something REALLY scary. When DVDs came out, people used their massive storage ability (at the time) to create **rainbow tables** of password hashes. I could explain rainbow tables but the Wikipedia does it so much better. Anyway, the new technology in the mix is Solid State Drives (SSDs). SSD seek times are crazy-fast, enabling rainbow-tables of IMMENSE size to be feasible. If the hacker has your password hash (as they might, if you were doing Windows NT-style authentication, or maybe even basic auth), then using an SDD-backed rainbow-table **they can crack a 14-character password in less than 5 seconds.** So you think your password **"(689!!!<>"QTHp"** is secure??? Think again!

I hate to say this, but I think passwords as a defense may have just gotten obsolete. What will we replace them with? Maybe some kind of **knuckle-recognition software.** :)

F5 Networks, Inc. | 401 Elliot Avenue West, Seattle, WA 98119 | 888-882-4447 | f5.com

F5 Networks, Inc.
Corporate Headquarters
info@f5.com

F5 Networks
Asia-Pacific
apacinfo@f5.com

F5 Networks Ltd.
Europe/Middle-East/Africa
emeainfo@f5.com

F5 Networks
Japan K.K.
f5j-info@f5.com