

Full-Disclosure: Re: [Full-Disclosure] Senior M\$ member says stop using passwords completely!

Re: [Full-Disclosure] Senior M\$ member says stop using passwords completely!

Source: <http://www.derkeiler.com/Mailing-Lists/Full-Disclosure/2004-10/0602.html>

From: Tim (tim-security_at_sentinelchicken.org)

Date: 10/16/04

To: RandallM <randallm@fidmail.com>

Date: Sat, 16 Oct 2004 10:46:44 -0400

> http://blogs.msdn.com/robert_hensing/archive/2004/07/28/199610.aspx

Jesus, that guy just doesn't get it, does he?

"Pre-computation attacks are a somewhat new and interesting phenomenon we are starting to encounter 'in the wild' through chainsaw security consultants. What they do is they pre-compute all of the possible LM or NT password hashes of a given length with a given character set and burn the pre-computed password-hash-to-password-mappings to DVD. Heck they can even submit their request to have your password hash reversed back into a password using a web page someone has setup to do the job for you (sorry, not going to give out THAT URL here.) . . . for free!"

Even if this was a new attack, a full rainbow table shouldn't be possible against a secure hash. Bottom line, M\$ dropped the ball, and has refused to pick it up.

"The LM hash is no longer cryptographically secure..."

When was it?

"Pass-phrase LENGTH, not complexity defeats these attacks."

Not if your hashes are chunked like some (all?) of M\$'s. Precomputed chunks with a good lookup table defeats longer passwords.

Mind you, I am no expert on M\$ "cryptography", but someone on their security team ought to know a bit more than this.

tim

Full-Disclosure – We believe in it.

Charter: <http://lists.netsys.com/full-disclosure-charter.html>

Re: [Full-Disclosure] Senior M\$ member says stop using passwords completely!