

FreeBSD-Security: Re: compare-by-hash (was Re: sharing /etc/passwd)

Re: compare-by-hash (was Re: sharing /etc/passwd)

Source: <http://www.derkeiler.com/Mailing-Lists/FreeBSD-Security/2004-09/0100.html>

From: David Schultz (das_at_FreeBSD.ORG)

Date: 09/28/04

Date: Tue, 28 Sep 2004 12:13:59 -0400

To: Colin Percival <cperciva@wadham.ox.ac.uk>

On Mon, Sep 27, 2004, Colin Percival wrote:

- > *If an appropriately strong hash is used (eg, SHA1), then the probability*
- > *of obtaining an incorrect /etc/*pwd.db with a correct hash is much*
- > *smaller than the probability of a random incorrect password being*
- > *accepted. Remember, passwords are stored by their MD5 hashes, so a*
- > *random password has a $2^{-(128)}$ chance of working.*
- >
- > *If, on the other hand, you're concerned about accidentally locking*
- > *yourself out of the server as a result of an undetected mangling of the*
- > *password database... you should be more worried about the server, and*
- > *all your backups, being simultaneously hit by lightning. :-)*

One thing to keep in mind is that the collision-resistance of SHA-1 is an unproven conjecture. Back in the dark ages of cryptography, Rivest conjectured that MD4 and MD5 were also collision-resistant, and this turned out not to be true. In fact, recent results have raised some concerns about SHA-1 (<http://eprint.iacr.org/2004/146/>). There's some speculation that SHA-1 is broken in the sense that you are likely to find a collision after computing far fewer than 2^{80} hashes; however, people still seem to consider it good enough for SSL/TLS and numerous other protocols. If they're wrong, of course, I think people will be much more concerned about digital signatures than rsync.

freebsd-security@freebsd.org mailing list

<http://lists.freebsd.org/mailman/listinfo/freebsd-security>

To unsubscribe, send any mail to "freebsd-security-unsubscribe@freebsd.org"