

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

**Source:** <http://www.derkeiler.com/Mailing-Lists/FreeBSD-Security/2004-09/0089.html>

---

**From:** Giorgos Keramidas ([keramida\\_at\\_freebsd.org](mailto:keramida_at_freebsd.org))

**Date:** 09/27/04

Date: Mon, 27 Sep 2004 12:17:10 +0300

To: Colin Percival <[cperciva@wadham.ox.ac.uk](mailto:cperciva@wadham.ox.ac.uk)>

On 2004-09-26 17:25, Colin Percival <[cperciva@wadham.ox.ac.uk](mailto:cperciva@wadham.ox.ac.uk)> wrote:

> *Giorgos Keramidas wrote:*

> > *After reading a nice paper by Val Henson[1] I'm not so sure I'd trust*

> > *sensitive information like password data to rsync without making sure*

> > *that compare-by-hash is disabled if at all possible.*

>

> *If you're going to disable compare-by-hash, you might as well just use*

> *rcp; but there's no theoretical justification for disabling*

> *compare-by-hash. Henson's paper points out a number of cases where*

> *hashing causes problems, but none of these are issues with hashing*

> *itself; rather, the problems arise from using hashing with an*

> *insufficient number of bits.*

Err, no.

Henson notes that since there's no absolutely guaranteed proof that there are *\*no\** collisions with a given hashing algorithm, comparing by hash value might result in two data blocks treated as identical even though they really are not.

Increasing the number of bits the hash key uses will decrease the possibility of a collision but never eliminate it entirely, AFAICT.

What I pointed out was that when a non-zero possibility of two data blocks comparing as equal (even though they are no) exists, the method in question should not be used for password data or other sensitive bits of information. A larger hash key will never yield a possibility of zero, so it doesn't mean that you can sleep untroubled at night while the rsync server overwrites /etc/\*pwd.db files periodically.

---

[freebsd-security@freebsd.org](mailto: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"