

Re: Password derived key with hash iterations

Source: <http://www.derkeiler.com/Newsgroups/sci.crypt/2003-07/2022.html>

From: Jed Davis (jdev_at_panix.com)

Date: 07/29/03

Date: Tue, 29 Jul 2003 12:11:14 -0400

cppdev9@yahoo.com (cppdev) writes:

- > *Hello,*
- >
- > *In some libraries I see a password deriving*
- > *function. It takes a hash iteration count.*
- > *Does iterating over original password's hash let's*
- > *say 100 times really gives any security?*
- > *It seems that all someone has to know to get the key*
- > *is the hash before the last one, am i missing something?*

The idea, I assume, is to make it harder to use a dictionary attack on the original password typed by the user. Guessing any of the intermediate stages should be as hard as guessing the eventual key, since with a good hash function they might as well be random bits.

Of course, if this 100x-hash isn't salted (some random bytes added to the password before hashing and included with the ciphertext), the attacker can precompute the 100x-hashes of their dictionary file and apply them to any ciphertext.

--

```
Jed Davis | "But life wasn't yes-no, on-off. Life was shades of  
<jdev@panix.com> | gray, and rainbows not in the order of the spectrum."  
<jldavis@cs.oberlin.edu> | -- L. E. Modesitt, Jr., _Adiamante_  
PGP key (fingerable) F33659F9 A098:903E:9B9A:DEF4:168F:AA09:BF07:807E:F336:59F9
```