

Re: Newbie question on encryption keys

Source: <http://www.derkeiler.com/Newsgroups/comp.security.misc/2007-07/msg00104.html>

- *From:* rgesw <nomail@xxxxxxxxxx>
 - *Date:* Sat, 28 Jul 2007 16:22:44 +0300
-

On Sat, 28 Jul 2007 02:01:26 +0200, Ertugrul Soeylemez
<do-not-spam-me@xxxxxxxxxx> wrote:

You have to assume that every attacker already has some information about you or your password. Probably he knows that you are using repetition patterns in all or many of your passwords, which makes attacking it much easier.

Quality of user passwords allows bad things. For example, one (quite typical) online site had average password entropy (strength) less than 15 bits. So, If users can and use that kind of lousy passwords, attacker has good chances for brute-forcing files without needing much of that extra information.

<http://groups.google.com/group/sci.crypt/msg/cfacf77ca70fd95b?&hl=en>

36ec2f330ba175cdc1aacbdcb812036c
83240670a27ad2bdc2c5a1b36222d3941aaf4bca
a2da3cafba3cd23391ad90511b7c7b73fa219492
64799812b5ee98a4cc1c6484bf8f849e3fee9aa6553393b9d7873b7f8cac9b825aca648a365aaa5e7037f903d708e19df219