

Re: Password Cracking

Source: <http://www.derkeiler.com/Newsgroups/comp.security.misc/2003-01/0534.html>

From: Ernst-Udo Wallenborn (ernst-udo.wallenborn@freenet.de)

Date: 01/24/03

From: Ernst-Udo Wallenborn <ernst-udo.wallenborn@freenet.de>

Date: 24 Jan 2003 23:07:54 +0100

"Mark H. Wood" <mwood@mhw.ULib.IUPUI.Edu> writes:

> *I think we have a case of violent agreement here. One side correctly*
> *points out that, *if all points in the keyspace have an equal*
> *probability of being chosen*, then decreasing the size of the total*
> *keyspace increases the chances of correct guessing. The other side*
> *correctly points out that *the observed behavior does not show an*
> *equal probability of choice over the entire keyspace* -- the portion*
> *of keyspace which is actually used is a very small subset of "all*
> *points", and argues that removing these highly popular points tends to*
> *disperse the actual choices.*

I violently agree.

--

Ernst-Udo Wallenborn