Q: *Just quickly read a bit about this Diceware; how is picking a few words myself different from using a dice and that diceware list? I'm probably missing something…*

A: Well, in principal there's no difference, *if* you can guarantee that the words you pick are truly drawn *with no correlation between them*, and come from a wider pool than is typical of normal conversation.

Most people, when asked, will choose words that have a pattern between them that correlates to their default language (verb adjective noun, adjective noun verb, whatever). They'll also often pick words from a list in their heads of only a few hundred words. The Diceware lists are 6^5 (7776) words long, and when drawn randomly result in (6^5)^4 unique 4-word passphrases. This is almost two orders of magnitude greater than the number of 8-character passwords drawn from the ~90 usable characters (Unicode offers some new and interesting options here, but current support is inconsistent at best). So a four-word passphrase is roughly as secure as a 9-character random password.

If you draw from a list of correlated words, or a small list that encompasses a sort of quotidian, workaday language, this no longer works very well. In other words, the list of *valid* four-word phrases in any language is much, much smaller than the list of all four-word permutations in that language.

An interesting question is what to do if Diceware randomly gives you a perfect English sentence like, “this is a great password”. I would tend to dump it and roll again, since removing the relatively small list of valid phrases has very little effect on the overall entropy, by definition.

Here is a randowm diceware generator

From:
https://www.astron.nl/lofarwiki/ - **LOFAR *Wiki***

Permanent link:
https://www.astron.nl/lofarwiki/doku.php?id=public:diceware_faq&rev=1492773326

Last update: **2017-04-21 11:15**