



Hidden Threats: Generated Passwords

How password generators potentially endanger IT landscape security

Jürgen Pabel, CISSP

Using identical passwords on multiple systems is common practice in today's IT world, but it exponentiates the potential damage in case such passwords are compromised; employing distinct passwords for all systems is very recommendable. But, the normal human capacity (actually: the willingness) for remembering passwords is usually very limited and users therefore employ some sort of password management tool: some write down their passwords on paper, others maintain text documents for storing their credential data; both practices are commonly very susceptible to compromise, thus most IT security professionals propagate the use of password management products.

Most password management tools offer not only secure storage for credentials, but they also relieve the user from having to produce random passwords via the power of imagination: the practically ubiquitous password generation feature. While this feature often increases password security many-fold, there is a hidden danger: if the password generator relies on a source of bad randomness for the generation process then generated passwords may become deducible. Determining the actual quality of randomness of generated passwords is possible for most practical means, but honestly: do you think (or know) whether your company evaluated any used password generator for this aspect?

Attackers may one day adapt their password cracking strategies to take advantage of the detailed issue:

- adding well known random passwords from flawed password generator implementations to password dictionaries further increases the chances of success for unfocused attacks;
- after encountering a compromised account that features a well known random password, targeting “related accounts” (same user - different system, etc) likely improves the chances of compromisation.

In closing, I want to restate that I am a proponent of password management products. They most often increase the often problematic state of password security in today's IT world. However, especially large IT environments may unwillingly expose their entire IT security if an employed password generation tool is found to be build on bad randomness.