Software Assurance Tips

A product of the Software Assurance Tips Team[2]

Jon Hood

Monday 16th August, 2021

1 The Password that Cannot Be Spoken

Updated Tuesday 10th August, 2021

To combat password reuse, several tools have been devised such as KeePass, 1Password, and Bitwarden. Even most web browsers now, like Google Chrome, can manage pseudorandom passwords that are reasonably strong and unique. Each of these tools provides a way to generate cryptographically secure random passwords, but there is an important limitation to these passwords that makes them a little less secure than they could be:

> The **pwgen** program generates passwords which are designed to be easily memorized by humans, while being as secure as possible. Human-memorable passwords are never going to be as secure as completely completely random passwords. In particular, passwords generated by **pwgen** without the **-s** option should not be used in places where the password could be attacked via an off-line brute-force attack.[3]

The goal of these password generation utilities is to generate passwords that can be written down, stored, and refernced. But are all passwords ones that fall into this category of pronouncability? Certainly not!

1.1 Password Categories

The majority of passwords are ones that may need to be communicated to someone. Passwords that are used for shared accounts and passwords that must be easily typed on a keyboard fall into this category. But there is another password category that we must consider: the temporary password.

Suppose that you are working for a technical support company, and a user calls claiming to have forgotten their password. They answer the security questions proving the first factor in authentication (something they *know*). You then send an encrypted e-mail with a temporary password that they must obtain via their recorded e-mail address (something they *have* access to).

There are few (if any) good reasons for these types of passwords (such as service accounts and temporary passwords) to be easily pronouncable, communicable, or typed in by a standard keyboard. To limit these passwords to such keyspaces decreases their security and increases the likelihood of shoulder surfers to obtain them.

1.2 A Solution for Temporary Passwords

Existing password utilities are inadequate for generating non-shoulder-surfable passwords. Therefore, I took the liberty of creating a new password generation utility: the Unspeakable PassWord GENerator (upwgen, `https://www.github.com/squinky86/upwgen/`). Upwgen works by generating at least a 15-character password[1, SV-222536r508029_rule] that includes characters in the following glyph blocks (using UTF-32):

- An uppercase letter[1, SV-222537r508029_rule]
- A lowercase letter[1, SV-222538r508029_rule]
- A number[1, SV-222539r508029_rule]
- A recognizable special character[1, SV-222540r508029_rule]
- A non-printing character
- An emoji
- A character in an extinct language
- A gamepiece

The emojis and gamepieces add to the keyspace of symbols for the password. The non-printing character makes it difficult to print out the password or write it on a sticky-note. And the extinct language means that characters from a language no one currently speaks will be included, making it difficult to communicate what the glyphs are.

1.3 Conclusion

Including symbols that are not easily typed and unprintable glyphs decreases the chance of a password being shoulder-surfed and increases the likelihood of a password being changed quickly, as it is not easy to simply write on a sticky note. The enlarged keyspace makes it less likely for a brute-force attack or rainbow table to contain the generated passwords.

References

[1] Application Security and Development STIG V5R1. Tech. rep. Oct. 2020. URL: https://dl.dod.cyber.mil/wp-content/uploads/stigs/zip/U_ASD_V5R1_STIG.zip.

[2] Jon Hood, ed. SwATips. https://www.SwATips.com/.

[3] Philipp Klaus. pwgen - generate pronouncable passwords. June 21, 2011. URL: https://raw.githubusercontent.com/jbernard/pwgen/master/pwgen.1 (visited on 08/09/2021).