Password Security: KeePass Password Safe

There are a number of recommendations that should be followed in order to use passwords securely. First of all a password needs to be sufficiently long and complex (i.e. drawn from a large set of characters) to make a brute force attack infeasible. Especially in the absence of rate-limiting or account blocking after failed attempts; such as when using poorly developed applications or if there is a possibility of an offline attack. [1] Secondly, dictionary words, common or previously compromised passwords, context related information (e.g. the website name), or easily obtained personal information (e.g. birthdays, phone numbers) should not be used to create a password. Otherwise the password would be vulnerable to dictionary attacks (a type of brute force attack where only likely possibilities are attempted). Finally the password should be kept private, never stored in a plain text file or written down. [2]

These requirements are further complicated by the importance of using unique passwords for different services. If one of these services were attacked and the password exposed, the attacker could gain access to any other services using the same password. There are many reasons why this could be possible, some examples include: An application that fails to properly implement password hashing, for example not using salt makes the passwords vulnerable to rainbow table attacks (using precomputed hashes). Or misconfigured server logging may capture and store passwords as plain text.

The more services that a person uses it becomes increasingly difficult for them to remember good unique passwords for each one. Research by Experian plc found that 'people have on average up to 26 online accounts protected by only five different passwords' [3]. In my personal experience I found that I was using the same password for countless different websites, all using the same email address. Therefore I decided that it was necessary to start using a password manager.

Using LDAPS for centralised authentication

asdf

References

[1] P. A. Grassi, J. L. Fenton, E. M. Newton, R. A. Perlner, A. R. Regenscheid, W. E. Burr, J. P. Richer, N. B. Lefkovitz, J. M. Danker, Y.-Y. Choong, K. K. Greene, and M. F. Theofanos, "Digital identity guidelines: Authentication and lifecycle management," Tech. Rep., Jun. 2017, Section 5.1.1.2, Appendix A. DOI: 10.6028/nist.sp.800-63b. [Online]. Available: https://doi.org/10.6028/nist.sp.800-63b.

[2] *Password recommendations.* [Online]. Available: https://security.web.cern.ch/security/recommendations/en/passwords.shtml.

[3] *Experian reveals the five key factors that make people & businesses more vulnerable to cyber fraud*, Dec. 2016. [Online]. Available: http://www.experian.com/blogs/news/2016/05/19/experian-reveals-five-key-factors-make-people-businesses-vulnerable-cyber-fraud/.