**A Comparison of Random Password Generators**

Kevin Barroga

Information and Computer Science 491

University of Hawaii at Manoa

Honolulu, HI, USA

kbarroga@hawaii.edu

*Abstract* — This paper describes the Diceware method for generating randomly chosen passwords or passphrases that are easy to memorize. It also compares the Diceware method with an Alpha Numeric password generating scheme in addition to user-chosen generated passwords with dictionary words. The security qualities and memorability of each method is discussed. Proposed changes to the original Diceware method to increase password memorability are discussed as well.

# Introduction

Passwords are still the most commonly used mechanism for user authentication in most computer systems. Alternative methods such as challenge-response, public-key, and biometrics are not very popular at the moment, and are often times combined with passwords. Password protection algorithms have evolved significantly. However, the common user is often the weakest link because they tend to choose predictable passwords that are easily guessed. Password cracking tools are readily available to perform brute force guessing attacks. Therefore, system administrators have tried to enforce stricter password restriction policies in an attempt to stop these attacks, such as requiring passwords to meet minimum complexity rules (minimum character length, at least one numeric, one non-alphanumeric, and one special character), or even require a frequent password changes.

Electronic commerce applications often use random generated passwords. E-commerce systems automatically generate passwords for users when they create new web accounts. Random passwords are also created and sent via email when old passwords are forgotten. High security systems such as military computers utilize random generated passwords [1]. Randomly generated passwords are commonly used for one-time authentication and for high security systems where the user is expected remember the password and is not to write it down.

Random generated passwords have significant benefits over user generated passwords. The key benefit is security. A randomly generated password guarantees that the password contains a specific amount of entropy. Entropy measures the unpredictability of a choice. This means that the generated password is chosen from a large set of passwords. When a user creates a password, it is unlikely that the password comes from a very large set. Users normally create simple passwords that are easy to remember, such as a common word combined with a number [2], [3]. For this reason, user-chosen passwords are much easier to attack than random passwords.

Some researchers have suggested users to create mnemonic phrase based passwords [4]. This suggestion is based on the idea that these passwords will not appear in password cracking tables and dictionaries, and will be less vulnerable to attacks. But Kuo et. al. revealed that a sophisticated attacker can build a password cracking dictionary for such passwords [5]. The passwords do not provide the necessary security like that of random generated passwords thus allowing a sophisticated password cracker to attack it as easy as word based passwords.

Another key benefit of random passwords is confidentiality. It is a common for people to use the same password for multiple web accounts and applications [6]. This makes it easy for an attacker to gain access to multiple accounts of a user. When an attacker compromises a weak website, he/she can learn the passwords for other websites. This practice of using the same password for multiple accounts creates a false sense of security of the user. A compromised website leads to a total loss of security. Random passwords increase security by forcing the use of unique passwords for different web accounts. There is still the risk of the user adopting the same random password for other web account which defeats the purpose of creating the random password.

Despite the benefits of random passwords, there are usability concerns. User generated password are easier to remember than random passwords. Users will choose passwords that have some meaning to them [6]. They create metal connections to the password so they can remember it. A random password has no inherent meaning to the user, making it difficult for them to memorize. Motivated users may use memorization strategies to build mental connections to remember the random password. Unmotivated users may not want to expend the energy, which may drive them to write down the password in plaintext and post it in plain view. Therefore it is important that a random password generator create passwords that are easy to remember.

The purpose of this paper is stated in the next section below. Related works follows. The original Diceware method is presented in the following section. The section after that will explain the experimental results. The final section presents the conclusion of this study.

# purpose

The purpose of this paper is to discuss the advantages of using the Diceware passphrase generator method compared to the Alpha Numeric method as well as user generated passwords. The security; amount of entropy in the passwords generated and the memorability; how easily a user can remember the passwords are used as metrics to compare the methods. Password length is not taken into account in this study. The password generating methods discussed in this paper can be modified to generate longer length passwords which would increase entropy. But the reluctant nature of the user remembering long password was taken into consideration, thus choosing to generate passwords of reasonable length. The AlphaNum method generates a sequence of random characters. The Diceware method creates passphrases of dictionary words. A proposed modification to the Diceware method, to help users create more memorable passphrases with little loss of security is discussed as well.

# Related Works

In Bunnell, et. al [7], they performed a similar study. They compared user generated passwords, randomly generated passwords, question-answer pairs, and word associations. They used a simple method of generating random passwords. It concatenated a three-letter word, and a numeral from 1-9, in addition to a four-letter word. Although the security of their password generating scheme was not complex, their study produced valuable experimental data. Participants in the study correctly remembered 70% of randomly generated passwords, and 77% of user generated passwords.

The United States Department of Defense has published guidelines for password management. They propose techniques for analyzing the security of passwords. They also present schemes which are similar to the AlphaNum and Diceware password generating schemes.

# Diceware method

The Diceware passphrase method [8], [9] was originally designed to be performed by hand using dice as random number generation. A set of n ordinary cubic dice are tossed and their numbers are used to pick a word from a table, called the dictionary. The Diceware method offers a few advantages [9]:

* Easy to understand and explain: it can be explained in a few sentences and make intuitive sense. The use of dice pedagogically stresses the importance of the randomness instead of psychological choice.
* Simple to implement in a computer: arguably the hardest part is the pseudo-random number generator; however, there are several good implementations widely available. The rest is a trivial table lookup.
* Generates easy to remember passwords: with a properly designed dictionary it is possible to “translate” the random numbers into common, words, making them easier to memorize.

The recommended setup uses a five dice toss per word, yielding = 7,776 possible values, which are also the number of word in the dictionary. Using the recommended five words, the size of the choice set is, yielding 64.62 bits of entropy. The Diceware wordlist however, is composed of words with different lengths ranging from one to six characters which results in passphrases ranging from five to thirty characters [9].

|  |  |
| --- | --- |
| Word Length | # of words |
| 1 | 51 |
| 2 | 748 |
| 3 | 853 |
| 4 | 2346 |
| 5 | 3111 |
| 6 | 631 |

This is the first weakness of the Diceware method. The variable length dictionary used by this method, have less entropy than a dictionary composed of fixed length words. Another drawback is that many of the words in the Diceware wordlist are not widely known English words, but numbers and symbols ex. “1930”, “60th”, “75%”, “86/3” etc.

# Password generating methods

*A. AlphaNum Scheme*

This scheme is the simplest password generator. It creates a random password that is six characters which alphabet includes upper-case letters, lower-case letters, and numerals 0 -9. The size of the alphabet is 26 + 26 + 10 = 62. The generator chooses from this alphabet six times. There are 62 possibilities for each character so the number of possible passwords is:

That is the size of the password set. It has 35.7 bits of entropy. Bits of entropy is a measure to compare the strengths of various password generators. This generator’s purpose is to create passwords that are short and can be recalled easily but also contain enough entropy.

|  |  |
| --- | --- |
| 1. z5mmZP | 11. UzE1Vt |
| 2. vueSPW | 12. GEd59t |
| 3. D1rjgj | 13. rwk0hk |
| 4. 0FloJf | 14. e3zC97 |
| 5. B3hds0 | 15. F38CKC |
| 6. f6fWgn | 16. W7TAtu |
| 7. 7aEpCl | 17. 5KnIjI |
| 8. fxpZwx | 18. rqcPrk |
| 9. VMwwDJ | 19. 0mcPJ8 |
| 10. L0lDVo | 20. Rn1tai |

*Output of AlphaNum Generator*

*B. Diceware Generator*

The Diceware generator produces a random list of words. It uses the principle of memorization and making mental connections. It uses the idea that forming mental connections to information may aid in memorization. People keenly remember words much easier than a string of random letters and numbers. People normally form mental connections to the meaning of a word. By creating passwords with words, the person can take advantage of existing mental connections to make memorization much easier. This kind of password that is formed with words is known as a passphrase. As stated in the previous section the creator of the Diceware method Reinhold provides a wordlist of 7776 common words.

Instead of using the recommended five words for generating a passphrase this generator chooses three words from the word list. That results in a password set of:

This method produces passphrases with 38.8 bits of entropy, gaining a slight advantage ahead of AlphaNum, which has 35.7 bits of entropy.

|  |  |
| --- | --- |
| 1. welt yarn dixon | 11. junky qx bless |
| 2. brood lower dinah | 12. wyeth tang reach |
| 3. same butch tansy | 13. soapy awoke bam |
| 4. frye round yet | 14. heckle yeasty halvah |
| 5. smack cv beam | 15. stage penal kz |
| 6. ug freer abbe | 16. psych faun fm |
| 7. mario : js | 17. abram suez randy |
| 8. silt 67th gy | 18. bemoan lingo howe |
| 9. wally moo bait | 19. indy dade slay |
| 10. 34th heroic joust | 20. ease abate city |

*Output of Diceware Method*

# Proposed Modified Diceware Method

The proposed changes to the original Diceware methods are: reduced dictionary size, and fixed length words. These two changes preserve the core of the Diceware method whilst addressing its shortcomings. The wordlist would be reduced to 6^4=1,296 words. The reduced dictionary size will make it easier to create a wordlist of common and familiar words. In addition to the smaller dictionary, words would be fixed to a limit of four characters only. This results in a standard passphrase of 24 characters, for fixed entropy.

This modified Diceware method brings a couple of advantages. First, fixed length words helps with memorization. If a user is unsure on whether a certain word is in singular or plural form, the user can depend on choosing the version with four characters because of the fixed length dictionary. Second, the dictionary will only contain alphabetic characters, enabling passwords to be typed quickly and proficiently [9].

Improved security can be obtained easily. The wordlist can be easily expanded to ensure extra security. A simple addition of a new word increases entropy at a rate of 10.34 bits per word. Another method to add security is by spicing the passphrase. Spicing is done by making small changes to the passphrase, like adding, deleting, or replacing characters which essentially removes it from the Diceware choice set. Random spicing would result in a much more password than user spicing. Normally when a user is asked to spice their password, most users would predictably change the letter “o”s by the number “0”s, or replace the letter “i”s with the punctuation “!”s. This is because people are not good at making random choices [9].

|  |  |
| --- | --- |
| 1. 1996 heed amid | 11. beam mare paul |
| 2. plod o'er wack | 12. ursa bolo note |
| 3. coma flux berg | 13. dyke vale 21st |
| 4. cuba i've bawl | 14. lest cowl 17th |
| 5. lump boyd honk | 15. oint whee bert |
| 6. curb noon trim | 16. over plus coco |
| 7. eden kiss fold | 17. love grab cope |
| 8. grab seat harp | 18. boor crib 9876 |
| 9. dddd tuff enol | 19. flea toni bird |
| 10. pogo 69th amen | 20. warm brew silt |

*Output of Modified Diceware Method*

# Conclusion

This study has shown that there is much room for improvement in generating random passwords. Modifications can be made to the password generators to create longer passwords with increased entropy. We also learned that users have a difficult time memorizing random passwords. Training methods for password memorization can be implemented to help users remember their passwords.

Improvements can be made to the AlphaNum generator by generating mnemonic aids. The Diceware dictionary can be improved by sifting out obscure words, numbers and symbols.

The set of modifications made to the original Diceware method make it easier to memorize, and use. The improvement of using fixed length words archives the same security to brute force attacks.

Security countermeasures against hardware and software keyloggers were not discussed in this paper. This may be an area discussed in future works.

# References

1. R. L. Brotman, *Department of Defense Password Management Guideline,* CSC-STD-002-85, Department of Defense Computer Security Center, 1985.
2. O Fredsite. (2006, November) End users attitudes and behaviours towards password management: Survey report. Dept. of Information Science, University of Otago, New Zealand. http://www.fredstie.com/thesis/survey/survey\_report.pdf
3. B. Schneir. (2006, December) Myspace passwords aren’t so dumb. Wired News. http://www.wired.com/news/culture/0,72300.html
4. D. V. Klein, ““foiling the cracker”: A survey of, and improvements to, password security,” in Proc. 2nd USENIX Security Workshop, 1990, pp. 5–14. http://www.klein.com/dvk/publications/passwd.pdf
5. C. Kuo, S. Romanosky, and L. F. Cranor, “Human selection of

mnemonic phrase-based passwords,” in *SOUPS ’06:* *Proceedings of the second symposium on Usable privacy and security.* New York, NY, USA: ACM Press, 2006, pp. 67–78. http://cups.cs.cmu.edu/soups/2006/proceedings/p67\_kuo.pdf

1. S. Gaw and E. W. Felten, “Password management strategies for online accounts,” in *SOUPS ’06: Proceedings of the second symposium on Usable privacy and security.* New York, NY, USA: ACM Press, 2006, pp. 44–55. http://cups.cs.cmu.edu/soups/2006/proceedings/p44\_gaw.pdf
2. J. Bunnell, J. Podd, R. Henderson, R. Napier, and J. Kennedy-Moffat, “Cognitive, associative and conventional passwords: Recall and guessing rates.” Computers & Security, vol. 16, no. 7, pp. 629–641, 1997.
3. Arnold G. Reinhold, The Diceware Passphrase Home Page, http://world.std.com/~reinhold/diceware.html
4. Carnut, M. A., & Hora, E. C. Improving THE Diceware Memorable Passphrase Generation System.
5. Leonhard, M. D. A Comparative Study of Three Random Password Generators.