



XXV Congresso de Iniciação Científica da Unicamp

18 a 20 Outubro Campinas | Brasil



Geração de senhas seguras com base no método Diceware

Leandro A. F. de Magalhães*, Diego F. Aranha

Resumo

O trabalho tem como objetivo aprimorar e adaptar o método Diceware para geração de senhas seguras e fáceis de se lembrar para o idioma português brasileiro. O método consiste em utilizar jogadas de dados e, com base nas faces obtidas, selecionar palavras de um dicionário contendo somente verbetes facilmente memorizáveis que comporão a senha.

Palavras-chave:

autenticação por senhas, método Diceware, idioma Português brasileiro

Introdução

As senhas constituem o método mais comum de autenticação há pelo menos 5 décadas¹, uma vez que oferecem várias vantagens.

Com isso, pôde-se encontrar as classes gramaticais e a composição das palavras que eram mais facilmente memorizáveis para criar um dicionário composto por elas.

	Sabe passwords, passphrases, PINs	Tem chaves, cartões de crédito	É digitais, reconhecimento facial
Custo	baixo	médio	alto
Flexibilidade	alta	baixa	impossível
Diversidade	alta	média	impossível

Figura 1. Comparação entre características de diferentes métodos de autenticação.

No entanto a lista das 25 senhas mais utilizadas por usuários em 2014 leva a conclusão de que o usuário muitas vezes opta por senhas facilmente memorizáveis, mas que apresentam baixa segurança.

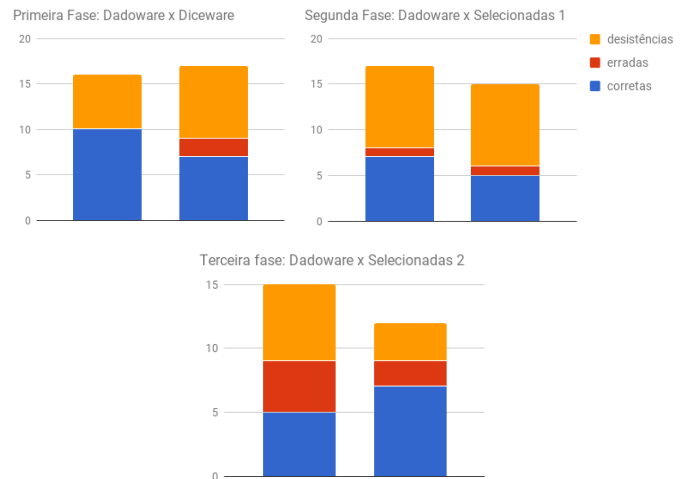


Figura 3. Resultados das 3 fases realizadas com conjuntos de palavras cada vez mais filtrados.



Figura 2. 10 piores senhas de 2014 de acordo com a SplashData.

Torna-se clara a necessidade de um método de geração de senhas mais seguras. O Diceware² é um desses métodos, apresentando um procedimento bem simples (amigável ao usuário) de ser seguido e uma alta segurança.

Resultados e Discussão

Foi realizada uma pesquisa de campo contendo várias fases - onde em cada fase um conjunto de palavras diferente foi utilizado para gerar e atribuir senhas aos usuários participantes, que deveriam voltar alguns dias depois para inseri-las.

Conclusões

Com base nos experimentos realizados, concluiu-se que um ótimo dicionário pode possuir as seguintes características:

- 1296 palavras (menos palavras significa uma melhor seleção), sendo substantivos, adjetivos e advérbios
- 4 a 7 letras (tamanho médio de 5.71 caracteres por palavra) e 2 a 3 sílabas

Um conjunto de palavras com essa característica foi gerado como dicionário final do trabalho.

Agradecimentos

Agradeço ao orientador Diego Aranha, à FAPESP, ao Instituto de Computação da UNICAMP, e a todos que participaram em alguma das fases da pesquisa de campo, que tornaram possível a conclusão do trabalho.

¹ Bonneau, J., et al.: Passwords and the Evolution of Imperfect Authentication, Communications of the ACM vol. 58 no. 7, July 2015.

² Reinhold, A.: The Diceware Passphraase Home Page, Disponível em: <http://world.std.com/~reinhold/diceware.html>