

Uma análise de padrões em senhas

Marino Souza S., Nilton V. C. Júnior, Luiz R. Rios

¹Instituto de Matemática – Universidade Federal da Bahia (UFBA)

{marino, niltonvasques}@openmailbox.org, luizromario@gmail.com

Resumo. *O método de adivinhação de senhas por força bruta necessita de um bom dicionário a fim de conseguir o maior número de adivinhações possíveis. Motivando-se no trabalho de [Li and Han 2014]. O presente artigo visa executar uma análise em cima de senhas web com o objetivo de encontrar padrões que futuramente sirvam para melhorar dicionário de adivinhação, ou desenvolver melhores políticas de senhas.*

1. Introdução

As bases de senhas utilizadas neste trabalho foram encontradas em sua maior parte no website SkullSecurity (<https://blog.skullsecurity.org/>) contendo senhas de provável usuários de língua inglesa, e outra base encontrada no PasteBin contendo um órgão de defesa de um governo de um país que neste trabalho será omitido o nome, algumas vezes utilizado o codinome: BrArmy. A quantidade de senhas totalizaram 64,493 provindas do SkullSecurity e 7,834 do BrArmy. Em ambos as bases de senhas haviam senhas em branco e com charset inválido que podem afetar as análises. Após a filtragem de alguns desses dados a quantidade total caiu para 64,463 da SkullSecurity e 7,833 da BrArmy. Durante este trabalho os autores preferiam utilizar o sistema internacional para representação de números reais e múltiplos de mil.

2. Estatísticas Comuns

fazer uma explicação da sessão.

	Skull leak	BR army
1	123456(0.202%)	12345678(4.864%)
2	password1(0.119%)	123456789(1.009%)
3	fuck(0.092%)	87654321(0.230%)
4	abc123(0.090%)	10203040(0.204%)
5	fuckyou(0.064%)	06121966(0.153%)

Table 1. Senhas mais usadas nas duas bases

Explicar oq a tabela 1 significa.

The abstract and “resumo” (if is the case) must be in 12 point Times font, indented 0.8cm on both sides. The word **Abstract** and **Resumo**, should be written in boldface and must precede the text.

2.1. Subsections

The subsection titles must be in boldface, 12pt, flush left.

	Exatamente Oito Dígitos	DDMMYYYY	MMDDYYYY	YYYYMMDD
Skull-leak	638(0.990%)	25.547%	5.799%	2.978%
BrArmy	3,565(45.513%)	26.928%	10.659%	0.701%

Table 2. texto da tabela

	Exatamente Seis Dígitos	DDMMYY	MMDDYY	YYMMDD
Skull-leak	1,066(1.654%)	36.210%	19.325%	11.445%
BrArmy	0%			

Table 3. texto da tabela

	Skull leak	BR army
1	password1(0.119%)	flamengo(0.115%)
2	fuck(0.092%)	exercito(0.115%)
3	fuckyou(0.064%)	infantaria(0.115%)
4	monkey(0.045%)	cavalaria(0.102%)
5	iloveyou1(0.043%)	guilherme(0.077%)

Table 4. Palavras Inglesas/Portuguesas mais usadas

2.2. sub

Curiosamente os usuário de língua inglesa preferem senhas relacionadas a palavras de baixo calão, como apresentado em 4, enquanto os usuário da base BrArmy recorrem em sua maioria a palavras que tem alguma relação as forças armadas.

2.3. sub

introdução da sessão.

	digit	lowercase	lowercase +digit	lowercase +symbol	digit +symbol	lowercase +digit+symbol	samerow
Skull-leak	6.15%	23.89%	56.93%	4.73%	0.08%	2.04%	0.64%
BrArmy	61.13%	11.44%	23.22%	0.09%	0.06%	0.26%	5.91%

Table 5. Composição das senhas.

3. Figures and Captions

Figure and table captions should be centered if less than one line (Figure 1), otherwise justified and indented by 0.8cm on both margins, as shown in Figure 2. The caption font must be Helvetica, 10 point, boldface, with 6 points of space before and after each caption.

In tables, try to avoid the use of colored or shaded backgrounds, and avoid thick, doubled, or unnecessary framing lines. When reporting empirical data, do not use more decimal digits than warranted by their precision and reproducibility. Table caption must be placed before the table (see Table 1) and the font used must also be Helvetica, 10 point, boldface, with 6 points of space before and after each caption.

4. References

Bibliographic references must be unambiguous and uniform. We recommend giving the author names references in brackets, e.g. [Li and Han 2014].

References

Li, Z. and Han, W. (2014). A large-scale empirical analysis of chinese web passwords. *23rd USENIX Security Symposium*, pages 558–574.