



# **An educational tool for password quality measurements**

**Author: Kirsi Helkala**

**Presentation: Patrick Bours**



# Content of the presentation

- Motivation
- Contributions
- The Quality Feedback algorithm
- Our tool
- Score limits
- Using tool in teaching
- Password policies among categories and some examples



# Motivation

- General instructions are too broad for all users
  - One remembers best meaningful passwords
  - One likes numbers and special characters
  - One recalls best patterns from the keyboard
- Online password generators claim to design strong passwords but can one really be sure?
- Memorability of the passwords
  - The users remember own-generated passwords better than computer-generated ones



# The contributions of the paper

- Three different password categories:
  - Non-word passwords, Mixture passwords, Word passwords
  - Different designing guidelines for each categories ([8])
- The educational tool
  - Helps users to design passwords by their own methods
    - Showing what makes passwords stronger
  - Evaluates the quality of the designed passwords by using a questionnaire
    - Actual password string is not needed to reveal



# Password categories

- Non-word passwords
  - Character strings, which do not contain any words
- Mixture passwords
  - Character strings containing both a word and a non-word part(s), e.g. "T!today65?"
- Word passwords
  - Strings which are either pure dictionary words, e.g. "password" or readable modifications of them e.g. "P@\$WORD"



# Words and modified words

Description	Example
Original dictionary word	library
Compound dictionary word	password
Reverse writing	yrarbil
Modifications with uppercase letters	LiBRaRy
Modifications with digits	l1brary
Modifications with special characters	l!br@ry
...	
Modifications with all sets	L1br@ry



# The Quality Feedback Algorithm

- Made by Conlan and Tarasewich [2]
- Uses simplified computations of the password search space
- The keyboard characters are divided into six groups
  - (lc, uc, d, shift digits, math characters, and other keyboard characters)and the entropy points are given based on the cardinality of the total group
  - Password containing only lowercase letters: each character is worth 26 points
  - Password containing both lowercase and uppercase letters: each character is worth 52 points (26+26).
- A repeated character gives only half of the character points
- E.g. "Password1"
  - Total 9 characters with 1 repeated character
  - $8(26+26+10) + (13+13+5) = 527$  points

[2] R.M. Conlan and P. Tarasewich. Improving Interface Designs to Help Users Choose Better Passwords. In *Proceedings of CHI 2006*, pages 652–657, Montral, Québec, Canada, April 2006. ACM Press.



## Our tool

- Based on the Quality Feedback Algorithm
  - Points computed similarly in the non-word part
  - We use only 4 groups (uc, lw, d, sc)
- Expands the idea by taking into account the words
  - The search space of the words is turned into the similar points than non-word part points
- Uses questionnaire to determine structure of a password



# Questionnaire

	How long is your password?
<b>W p</b>	How many words does your password contain?
<b>O a</b>	What languages are the words based on?
<b>R r</b>	How many letters does the 1 <sup>st</sup> , ..., nth word contain?
<b>D t</b>	How many uppercase letters are there?
<b>-</b>	How many digits are there?
	How many special characters are there?
<b>N W</b>	How many upper case letters are there?
<b>O O</b>	How many lower case letters are there?
<b>N R</b>	How many digits are there?
<b>- D</b>	How many special characters are there?
	How many reused characters are there?



## Example answers: 1Sv@r!

	How long is your password?	6
<b>W p</b>	How many words does your password contain?	1
<b>O a</b>	What languages are the words based on?	Nor
<b>R r</b>	How many letters does the 1 <sup>st</sup> word contain?	4
<b>D t</b>	How many uppercase letters are there?	1
<b>-</b>	How many digits letters are there?	0
	How many special characters are there?	1
<b>N W</b>	How many upper case letters are there?	0
<b>O O</b>	How many lower case letters are there?	0
<b>N R</b>	How many digits are there?	1
<b>- D</b>	How many special characters are there?	1
	How many reused characters are there?	0



# Our tools computations briefly

- Quality Score = Non-word part + Word part
- Non-word part =  $(l_{nw} - 0,5re)(c_{UC}29 + c_{LC}29 + c_D10 + c_{SC}37)$ 
  - $l_{nw}$ : the length of the non-word part,  $re$ : the number of the reused characters,  $c$ : 1 if the set is used, 0 if not
- Word part contains pure dictionary words points and modification points
  - Pure dictionary words: the entropy of the words written with lowercase letters
  - Modifications done with: the entropy of the combinations when a word is modified with uppercase, digits, and/or special characters



# Our tools computations briefly

$$\text{Word Part} = \begin{cases} \text{PureWord} + \text{Modification}, & \text{PureWord} > \text{Modification} \\ \frac{\text{PureWord}}{\text{Modification}} \text{PureWord} + \text{Modification}, & \text{otherwise} \end{cases}$$

$$\text{PureWord} = \frac{\log_2 \prod_{i=1}^n \text{NW}(l_i)}{\log_2(29^{wch})} \times 29^{wch}$$

$$\text{Modification} = \frac{\log_2 \binom{wch}{uc} + \log_2(10^d) + \log_2(37^{sc})}{\log_2 \left( \binom{wch}{uc} 29^{uc} \binom{wch-uc}{d} 10^d \binom{wch-uc-d}{sc} 37^{sc} 29^{lc} \right)} \times \text{AllCases}$$

$$\text{AllCases} = (c_{UC} 29 + c_{LC} 29 + c_D 10 + c_{SC} 37) wch - \text{PureWord}$$

- **NW**: the number of dictionary words with the length  $l_i$
- **n**: the number of the words in the password
- **wch**: the number of the word characters
- **uc**: uppercases
- **lc**: lowercases
- **d**: digits
- **sc**: special characters
- **c**: 1 if the set is used, 0 if not



# Score Limits

- A good password:  $> 735$  points
  - The revealed information (the adversary knows the answers of the questionnaire) about the password structure in bits is less than half of the baseline bits (94 bits)
  - Based on the computations done in [8]
- A strong password:  $> 875$  points
  - Search space entropy is higher than 56 bits
  - Based on the definitions done in [7]



# Teaching to design good passwords

- A tutorial session is needed
  - Users are explained different password categories and their own password designing processes are discussed
  - Current password generation processes are evaluated based on the quality points of the current passwords
  - The users are taught how to generate good passwords within each three password categories
    - Different tricks (mnemonic phrases, keyboard encryption, etc.)
    - What ever trick is used, the designed passwords should satisfy the policy of the password category it belongs
- Afterwards the tool can be used by users alone



# A good Word passwords

- Longer than 12 characters
- Based on many short words
- Used words are modified with characters from all character sets
- Needed to be mentioned:
  - Modification should be done differently in each password designing session
  - Avoid using words from the same theme



# Building a good Word password

Password	Description	Score
<b>Skaløyahosfar</b>	13 lowercase letters, 4 words	<b>288</b>
<b>\$K@1#y@H0\$f@R</b>	Modified with 3 uppercase letters, 2 digits, and 6 special character	<b>749</b>



# A good Mixture password

- Longer than 10 characters
- Based on short words are used
- Used words are modified
- Contains special characters and digits between the word parts
- Needed to be mentioned:
  - Vary placements of the word and non-word parts
  - Vary modification style of the words
  - Avoid using words from the same theme



# Examples of Mixture passwords

Password	Description	Score
<b>E&gt;regn&amp;*:-o</b>	Based on "Jeg elsker regn og sol" 1 word: no modifications non-word: 1 lc, 1 uc, and 5 sc	<b>745</b>
<b>EeSn#&amp;S0l3!</b>	Based on "Jeg elsker snø og sol" 2 words: modified with 2 uc, 1 d and 1 sc non-word: 1 lc, 1 uc, 1 d, and 2 sc	<b>808</b>



# A good Non-word password

- Longer than 8 characters
- All character set should be used
  - By using longer passwords it is not necessary to use characters from all groups
- Needed to be mentioned
  - Avoid using commonly known mnemonic phrases such as “To be or not to be”
  - The best phrases are only meaningful to the user
  - Same goes for the other memorizing models
  - Avoid using same characters in each password designing session



## Examples of Non-Word passwords

Password	Description	Score
<b>2(3+4i)=A</b>	9 characters, all character groups, a math formula	<b>945</b>
<b>IwG'sA@9.40</b>	11 characters, all character groups, mnemonic phrase: "I watch Grey's Anatomy at 9.40"	<b>1155</b>
<b>;oyy2Åsdd3Ptf</b>	Keyboard encrypted from "Mitt1Pass2Ord"	<b>1312,5</b>



**THANK YOU!**

**QUESTIONS?**



## Mentioned references

- [2] R.M. Conlan and P. Tarasewich. Improving Interface Designs to Help Users Choose Better Passwords. In *Proceedings of CHI 2006*, pages 652–657, Montral, Québec, Canada, April 2006. ACM Press.
- [7] K. Helkala and E. Snekkenes. A method for ranking authentication products. In *Proceedings of the International Symposium on Human Aspects of Information Security & Assurance (HAISA 2008)*, July 8-9, Plymouth, UK, 2008.
- [8] K. Helkala and E. Snekkenes. Password generation and search space reduction, June 2008. Submitted for publication.