Password security

Kinds of passwords

- Password
  - A string of characters: A,B,C,…d,e,f,…1,2,3…!,”,@,…
- PIN-code
  - A string of numbers
- Pass phrase
  - A sentence
- Associative and cognitive passwords
  - Answers to the questions
  - Associative, cue words
    - Black: white, strawberry: blueberry, dad: mum, day: night etc.
  - Cognitive
    - What is your second name? How many cats do you have? Which chocolate you like best?
- Pass face, pass image

Password space - S

- S is the total set of all passwords
- Size of S is denoted by s
- 4-digit PIN codes: $s = |S| = 10^4$
- 6 character passwords:
  - $s = 26^6$
  - $s = 52^6$
  - $s = 62^6$
  - $s = 94^6$

The art of counting

- Number of possibilities with one dice: 6
- Number of possibilities with two dices:
  - Unordered: 21
  - Ordered: 36
- Number of 5 letter combinations: 26^5
- Including capitals: 52^5
- Including numbers: 62^5
- All keyboard symbols: 94^5

Combinatorics - 1

- We will count the number of 6 character passwords
  - All is possible: letters, capitals, numbers and special characters
  - If no restriction, then we have 94^6 possible passwords
- On the next slides we will introduce specific restrictions

Combinatorics - 2

- At least 1 number?
  - Total number of 6 character passwords: 94^6
  - Number of 6 character passwords <u>without</u> numbers: 84^6
  - Answer: $94^6 - 84^6 = 338.571.749.440$
- Trick: All – those that are wrong

Combinatorics - 3

- Have 6 different characters?
  - First character: 94 possibilities
  - Second character: (94-1) possibilities
  - Third character: (94-2) possibilities
  - Answer: 94*93…*89 = 586.236.072.240 =
- Trick: Count every time what is still possible

Combinatorics - 4

- At least 1 capital and 1 number?
  - No restrictions: 94^6
  - No capitals: 68^6
  - No numbers: 84^6
  - No capitals and no numbers: 58^6
  - Answer: $94^6-68^6-84^6+58^6 = 277.772.959.360 = 2^{38,02}$
- Trick: All – wrong ones + those subtracted twice!

Combinatorics – 5

- Exactly 1 number?
  - Choose position where the number will be: 6 possibilities
  - Number on that position: 10 possibilities
  - All other 5 positions: (94-10) possibilities
  - Answer: $(6*10) * 84^5 = 250.927.165.440$
    Trick: Place number first.

Combinatorics - 6

- Exactly 1 number and exactly 1 capital?
  - Choose position for the number: 6 possibilities
  - Number on that position: 10 possibilities
  - Choose position for the capital: (6-1) possibilities
  - Capital on that position: 26 possibilities
  - All other 4 positions: (94-10-26) possibilities
  - Answer: $(6*10) * (5*26) * 58^4 = 88.268.668.800$
- Trick: Place number and capital first

Combinatorics - 7

- Exactly 2 numbers?
  - Choose 2 positions for the numbers:

    6*5/2 = 15 possibilities
  - Numbers on those position: 10 possibilities
  - All other 4 positions: (94-10) possibilities
  - Answer: $15*10^2 * 84^4 = 74.680.704.000 =$

Combinatorics - 8

- Choose 2 positions for the numbers gives 15 possibilities. Why?
- "Choose m out of n":

  n! / (m! * (n-m)!)

  - k! = 1*2*…*(k-1)*k
- "Choose 2 out of 6": 6!/(2!*4!) = 15

Probabilities

- What is the probability that a random password of 6 characters has no number in it?
  - Answer: $84^6 / 94^6 = (84/94)^6 = 0{,}509$
  - So approximately have of the 6 character passwords does not have a number in it!
- In general is the probability equal to the size of set of correct answers divided by the total number of answers.

Good Properties

- **Hard to guess**: do not use names, dates, telephone numbers, etc.
- **Easy to remember**: no need to write it down or share with other persons
- **Private**: otherwise no authentication possible
- **Secret**: owner is the only one who knows it

Attacks

- Dictionary attack
- Not fooled by
  - Capitals
  - Change of letters into numbers
  - Permutations
- What can we do?

To not do list - 1

- PW based on user's account name
- PW which match a word (or reversed word) in a dictionary, regardless if some or all of the letters are capitalized
- PW which match a word in a dictionary with an arbitrary letter turned into a control character

To not do list - 2

- PW which are simple conjugations of a dictionary word (i.e. plurals, adding “ing” or “ed” to end of word, etc.)
- PW which do not use mixed upper and lower case, or mixed letters and numbers, or mixed letters and punctuation

To not do list - 3

- PW base on user's initials or given name
- PW which match a dictionary word with letters replaced by numbers (eg '3' for 'e')
- PW which are patterns from the keyboard (eg. "aaaaa" or "qwerty")
- PW which only consist of numbers

The PROBLEM!

- We have limited memory
  - Can only remember 7±2 totally random symbols
- Even more problems when
  - We have multiple passwords
  - We need to change passwords regularly

What can we do – part 1?

- Pass phrase
  - Yesterday I watched a nice program on television.
  - YIwanpot or Y1wanp0t
- Use events on news or personal events when forced to change regularly

What can we do – part 2?

- Encryption
- Shift every character fixed number of positions
- Shift every character by increasing number of positions

- http://geodsoft.com/cgi-bin/pwcheck.pl

Pass faces and images

- It is easier to recognize then to remember.
- Setup:
  - Memorize a set of selected or given pictures
- Authentication:
  - Recognize memorized pictures

Pass faces

- Five faces are presented and need to be memorized
- Five 4x4 grids are presented each containing 1 memorized image