Password security

Dr.Patrick A.H. Bours

Password: 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:
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:
  - $s = 26^6$
  - $s = 52^6$
  - $s = 62^6$
  - $s = 94^6$

Password: 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

Password: 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

Password: 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

Password: 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

Password: Combinatorics - 4

- At least 1 capital <u>and</u> 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!

Password: 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.

Password: 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

Password: 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 =

Password: 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

Password: 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.

Password: Statistics - Introduction

- Let $\mathbf{x} = (x_1, x_2, \ldots, x_n)$ and $\mathbf{y} = (y_1, y_2, \ldots, y_n)$ be two equally long sequence of numbers.
- Let p_i be the probability that occasion x_i occurs.
- $p_1 + p_2 + \ldots + p_n = 1$

Password: Statistics - Mean μ

- The mean of **x** is the *weighted average* of the values of **x**. The weights are the probabilities.
- Also called "Expected value"
- $E(\mathbf{x}) = \mu_{\mathbf{x}}$
- The mean $\mu_{\mathbf{x}}$ of **x** is defined as:

$$\mu_{\mathbf{x}} = p_1x_1 + p_2x_2 + \ldots + p_nx_n$$

Password:
Statistics - Mean μ - example

- Values of a dice: $\mathbf{x} = (1,2,3,4,5,6)$
- True dice: $\mathbf{p} = (1/6,1/6,1/6,1/6,1/6,1/6)$
- $\mu_{\mathbf{x}} = (1+2+3+4+5+6)/6 = 3.5$

Password: Statistics - Variance σ^2

- The variance is a measure of how much the members of **x** are scattered around their mean.
- The variance $\sigma_{\mathbf{x}}^2$ of **x** is defined as:

$$\sigma_{\mathbf{x}}^2 = V(\mathbf{x}) = E(\mathbf{x} - \mu_{\mathbf{x}})^2 =$$
$$= E(\mathbf{x}^2) - 2\,\mu_{\mathbf{x}}\,E(\mathbf{x}) + (\mu_{\mathbf{x}})^2 =$$
$$= E(\mathbf{x}^2) - (\mu_{\mathbf{x}})^2$$

Password: Statistics - Covariance $\sigma_{\mathbf{xy}}$

- We use covariance to measure similarity between **x** and **y**.
- $\sigma_{\mathbf{xy}} = E((\mathbf{x} - \mu_{\mathbf{x}}) * (\mathbf{y} - \mu_{\mathbf{y}}))$

Password: Statistics - Correlation ρ_{xy}

- $\rho_{xy} = \sigma_{xy} \, / \, (\sigma_x * \sigma_y)$
- If $\rho_{xy} = 0$ then **x** and **y** are uncorrelated.
- The larger $| \rho_{xy} |$ is, the more **x** and **y** are correlated.
- Sign of ρ_{xy} tells something about *direction* of correlation

Password: Entropy - h

- Entropy h is a measure of the randomness
- Entropy h is the number of bits needed to describe the members of S
- In formula:
  - $h = \log_2(s)$
- Assumption: all passwords are equally likely

Password: Examples of entropy

- 4-digit PIN code:
  - $s = 10^4$
  - $h = \log_2(10^4) = 13,3$
- 6 character password
  - $s = 94^6$
  - $h = \log_2(94^6) = 39,3$

Password: Entropy – more complicated

- Let $S = \{s_1, s_2, \ldots, s_s\}$
- Let $P = \{p_1, p_2, \ldots, p_s\}$, where p_i is the probability someone uses password s_i
- Entropy is now defined as:
  - $h = -p_1\log(p_1) - p_2\log(p_2) - \ldots - p_s\log(p_s)$

Password: Entropy – more complicated

- If $p_i = 1/s$ for all i then:

- h = -1/s log(1/s) - … - 1/s log(1/s) =

  = -s * 1/s * log (1/s)

  = -log(1/s) = log(s)

- So definitions are consistent

Password: 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

Password: Attacks

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

Password:
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

Password: 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

Password:
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

Password:
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

Password: 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

Password:
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

Password: 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

Password: Pass faces

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

Password: Pass images

- p (random) images selected and remembered
- n images presented containing m selected images

- Vary value of m during authentication
- Present more challenges

Password: References

- R. Smith, **Authentication: From Passwords to Public Keys**, Addison-Wesley, 2002.
- J. Yan, A. Blackwell, R. Anderson, and A. Grant, **Password Memorability and Security: Empirical Results**, IEEE Security & Privacy Magazine, Vol. 2, No. 5, Sept/Oct 2004, pp. 25-31.
- L. O'Gorman, **Comparing Passwords, Tokens, and Biometrics for User Authentication**, Proceedings of the IEEE, Vol. 91, No. 12, Dec 2003, pp 2019-2040.
- http://www.passfaces.com
- http://www.sims.berkeley.edu/~rachna/dejavu/