Cryptography, winter 2014/2015

PD Dr. Adrian Spalka, Dr. Daniel Loebenberger

2. Exercise sheet
Hand in solutions until Saturday, 08 November 2014, 23:59:59

Exercise 2.1 (Security policies). (6 points)

Determine the values and how they have to be protected for two information systems in the following environments:

(i) a social network, $\boxed{2}$

(ii) a university administration, $\boxed{2}$

(iii) a hospital. $\boxed{2}$

Which of the aspects of a derived security policy would be mandatory (where specified?) and which would be at digression (whose?)?

Exercise 2.2 (Trusted third parties). (8 points)

(i) Find examples for an IS-architecture and a communication structure, whose security depends on the cooperation of a trusted third party. $\boxed{2}$

(ii) Analyze the role of these parties with respect to outsourcing and cloud computing. $\boxed{2}$

(iii) Write down in detail your fundamental thoughts on the claim "Trusted third parties considered harmful."[1] $\boxed{4}$

Exercise 2.3 (Secure passwords). (7+5 points)

Consider password with ℓ letters, where each letter was uniformly selected from an alphabet A.

(i) Compute the required length ℓ such that any password generated uniformly at random has at least 80 bits of security, where $\boxed{2}$

[1] "XY considered harmful" used to be a popular title, whenever the invention XY was not considered an improvement anymore.

(a) $A = \{0, \ldots, 9\}$ are the Arabic numerals.

(b) $A = \{a, \ldots, z, A, \ldots, Z\}$ are case-sensitive roman letters.

(c) A are all 94 ASCII printable characters (excluding space).

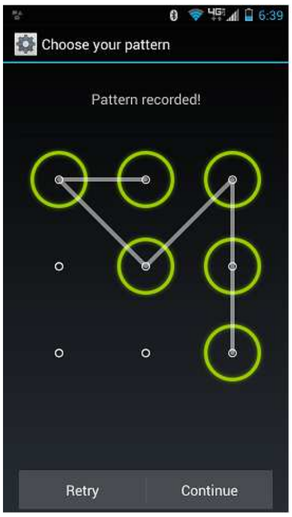
(d) A is a Diceware word list as found on our course webpage.

$\boxed{5}$ (ii) For one of the above alphabets generate such password. Describe detailed how you proceeded and argue why you think the result is indeed drawn uniformly at random from all admissible passwords.

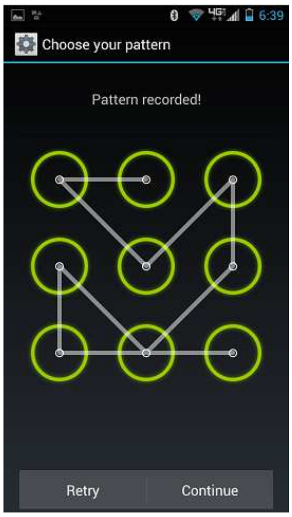
$\boxed{+5}$ (iii) Generate a human selected password with 40 bits security. Follow here the estimates from NIST Special Publication 800-63, Appendix A, available on our course page.

Exercise 2.4 (The entropy of Android swipe-patterns). (0+5 points)

$\boxed{+5}$ In order to access a modern Android device, the user has to paint with his fingers a pattern over a three times three grid. If the pattern matches the stored one, the device is unlocked.


Choose your pattern

Pattern recorded!


Choose your pattern

Pattern recorded!

Your task is to estimate the entropy of a randomly selected swipe-pattern with ℓ swipes for $\ell = 2, \ldots, 8$. Hint: The pattern starts at any of the nine positions. Assume then for simplicity that the pattern continues at any *adjacent* grid-point, where also diagonal movements are allowed. Compute the average number of possibilities for moving to another grid point and use it to estimate the entropy of each additional swipe.