EECE 412, Fall 2009

Quiz #3 Key

This quiz consists of 4 pages. Please check that you have a complete copy. You may use both sides of each sheet if needed.

Your Family name: _____

Your Given name: _____

Your student ID: _____

#	Points	Out of
1		7
2		4
3		4
TOTAL		15

Name of your left neighbor: _____

Name of your right neighbor: _____

ATTENTION: When necessary, make reasonable assumptions and state them clearly in your solutions.

1. **Strength of your password.**
   a. **(1 point) Assume that your online banking password is "6LopxHi!". Indicate below how many low case, capital case, digits, and special characters it has.**

Number of alpha characters in your password	6
Number of special characters, e.g.,)[!(#@$%^&~;:",.+_-`}{]\/?, in your password	1
Number of numeric characters in your password	1
Total number of characters in your password	8

   b. **(2 points) Compute <u>theoretical</u> entropy of the password. State clearly your assumptions about the size of the special character space and any other assumptions. Explain your answer.**

Possible helpful reminder: $\log_b(x) = \frac{\log_k(x)}{\log_k(b)}$.

Assumptions: 26*2= 52 alpha characters, 26 special characters, 10 numeric characters.

Theoretical entropy of the above password is $\ln_2((52+26+10)**8) = 8\ \ln_2(88) = 8*6.5 = 51.7 \approx 52$ bits

   c. **(2 points) Compute <u>effective</u> entropy of the password. State clearly your assumptions about the size of the special character space and any other assumptions. Explain your answer.**

Possible helpful reminder: $\log_b(x) = \frac{\log_k(x)}{\log_k(b)}$.

Assumptions: 26*2= 52 alpha characters, 26 special characters, 10 numeric characters.

Effective entropy of the above password is $\ln_2((52**6)*26*10) = 6\ \ln_2(52) + \ln_2(26) + \ln_2(10) = 6*5.7+4.7+3.3 = 42.2 \approx 42$ bits

d. (1 points) How long, on average, will it take for an attacker to "crack" your password if she can use her computing resources to test 2^21 candidates per second? Consider only the theoretical entropy of your password. Explain your answer. Assume that your password hash is salted.

(2**(52-1))/(2**21) = 2**30 seconds = 2,147,483,648/3600/2 = 596,523 hours = 12,428 days, which is little bit over 34 years.

e. (1 points) How long, on average, will it take for an attacker to "crack" your password if she can use her computing resources to test 2^21 candidates per second? Consider only the effective entropy of your password. Explain your answer. Assume that your password hash is salted.

(2**(42-1))/(2**21) = 2**20 seconds = 1,048,576/3600 hours = 291 hours = 12 days.

2. **Assuming the attacker cannot perform an off-line dictionary attack, list the techniques that your bank can employ for reducing the chance of your account being compromised through an on-line dictionary attack?**

   - Exponential back-off
   - Disconnection
   - Account disabling
   - Jailing
   - Two-factor authentication

3. **Compare and contrast ACLs and capability lists.**

   - In ACL-based systems, it's easier to list all the users who have access to a resource. Whereas in capability systems, it's easier to review all the resources that a user has access to.
   - Capabilities are easier to delegate than rights in ACLs.
   - Capability delegation and forgery are difficult to control and prevent.