**CSC 301 Lab 01: IDs, Passwords, and Authentication**

Points: **100** points.

**Format:**

* File type: Word file (.doc or docx).
* File name: LastName\_FirstName\_Lab01
  + e.g. Bond\_James\_Lab01.doc
  + Add your name also as a header as seen with assignment title.
* Font: Times New Roman.
* Font size: 10.
* Page number: at the bottom.
* Line and Paragraph Spacing: 1.0

**Rules:**

* Keep it short, keep it simple.
* No long paragraphs or essays.
* Please answer systematically using short itemized bullets.
* Simply write the question number followed by the answer.
* *You will lose points up to %10 not following the exact format rules explained above.*

1. [15 points] Can we use the legal system (Laws, regulations, Police forces, Prosecutors, etc.) to protect computer systems? Support your answer with *three* reasons.

Yes, we can by many means.

* Using copyright laws we can protect rights to certain products that is unique to you.
* By using many different types government agencies (FBI, CIA, etc.) it can protect against foreign threats.
* There can be many regulations that can be used so that younger people who “happen” to access information or websites that they aren’t supposed to and end up get some sorts of hostile virus, should be monitored vigorously.

1. [15 points] When police investigators perform DNA analysis are they doing *identification* or *authentication*? And why? Explain your answer.
   1. They are doing identification. This is identification because they have not yet have come to an answer or prime suspect. If they were doing a authentication it is to prove if something is true or not.

1. [25 points] Describe A dictionary attack can be augmented to try orthographic substitutions, such as 2 for z and @ for a. Assume a common dictionary has 100,000 words and (to make calculations easy), all letters are lower case and the 26 letters are evenly distributed (that is, “a” occurs exactly 1/26 of the time as does “z”). How many extra substitute word possibilities are there, allowing @ for a? (That is, the attack would try the word “bay” and also “b@y”.) If there are ten such orthographic substitutions (2 for z, @ for a, 1 for I, 6 for b, $ for s, etc.), how many word possibilities would an attacker need to try?
   1. In the 100,000 possibilities where there are a equal amount of each of the 26 letter words. Then there are approximately 10 symbols so we can do 100,000 \*(1/10) + 100,000 = 110,000.

1. [15 points] If a user is prohibited from using any of the most recent *n* passwords, why should the system still protect those passwords from viewing, just as strongly as it protects the current password? Give *three* reasons.
   1. It is to protect the user from outsiders who might be able to access your old passwords and find patterns and similarities in turn guessing or predicting the new password.
   2. It is so that you don’t use a variation of the password in another way. For example ILOVEDONUTS to 1L0V3D0NUT5 which is obviously not safe.
   3. Lastly it is because for most people it is common to have used a password more than once.

1. [15 points] Discuss the security impact of a biometric device that sends simply “yes” or “no” to the computer to show the user passed or failed authentication, versus one that sends a full representation of the biometric credential to be evaluated on the computer. For example, a user might insert a coded card (with his or her biometric pattern secretly encoded) into a reader and then place a finger over a print reader. The reader can then inform the computer that the user did or did not match the pattern described on the coded card.

The security impact varies in many ways between the two circumstances where both have their pros and cons.

Pros for a simple yes or no to show if the user passed or not the pros: much faster, less work and memory

Cons: the security is less secure than the alternative which needs a full representation.

Pros for the full representation : More secure, more reliability.

Cons: Longer, more energy and data.

1. [15 points] Must identities be unique? Must authentication data be unique? Explain your answer.
   1. To my understanding identities are either user-id or email-id so they may not be unique since they are one part of a key to access something. While authentication data does have to be unique since it is the process to prove whether something is true or not, so it is best for it be unique for maximum security.

**- The End -**