School of Computing & Information Technology

CSCI862 System Security
Spring 2016

Assignment 1 (12 marks, worth 12%)

Due 11:59pm Saturday 20^{th} August 2016.

Part One: Short answer questions: 4 Marks

1. A phonetic segment generator works as follows. Each segment has 3 English letters. The form of each segment is $\Delta\Phi\Delta$ (consonant, vowel, consonant), where Φ is an element in {a, e, i, o, u} and Δ is an English letter which is not in {a, e, i, o, u}. Determine the entropy associated with the following method of generating a password. **1 Mark**

   > Choose, and place in this order, one phonetic segment cosisting of lower case letters, followed by three digits and then two symbols drawn from the set {+,*,@,#,$}. Finally, apply `Whirlpool` to give an output string in hex which will be used as a password.

   You should assume the random choices are made with equal likelihood of each symbol from the space being chosen. So for a random digit there are 10 possibilities each of which is chosen with probability 1/10.

   ***

   Total number of possible passwords $N = 21 * 5 * 21 * 1000 * 5 * 5 = 55,125,000$

   Each of these is mapped to a password by ther hash function Whirlpool. The mapping itself is deterministic so there is no uncertainty so no additional entropy is obtained. If there are collisions the number of passwords may actually decrease so hashing may decrease the entropy.

   Entropy: $log_2 N = 25.72$.

2. Consider the following statements and answer the subsequent questions:

   ```
   Alice can climb walls and jump fences.
   Bob can push walls and push doors.
   Chris can push Alice, push fences and jump walls.
   Dan can open doors and jump Alice.
   ```

   (a) What are the subjects, objects and actions for this scenario? **0.25 Mark**

(b) Draw an access control matrix representing this scenario. **0.25 Mark**

*** Subjects: Alice, Bob, Chris, Dan Objects: walls, fences, doors, Alice Actions: climb, jump, push, open

Table 1: Access Control Matrix

	walls	fences	doors	Alice
Alice	climb	jump		
Bob	push		push	
Chris	jump	push		push
Dan			open	jump

3. Consider the lattices in the file `A1-Q3.pdf` and answer the questions below. A line going down from level X to level Y indicates that level X dominates level Y. Assume this diagram is with reference to BLP. For the questions other than the first you can work with whichever of the diagrams you feel most comfortable with. Justify your answers.

   (a) How are the diagrams A and B related as lattices? **0.25 Mark**
   ***These are equivalent lattices. There is a 1-1 mapping between the nodes in each such that there is the same domination relationships.

   (b) I have one object at level 1010 and another object at 0001. What is the most appropriate level for a subject to be assigned so both objects can be read by the subject? **0.25 Mark**
   ***For the subject to be able to read the object it needs to be at a level that dominates the specified levels, but doesn't dominate any other levels that dominate both. In other words, we want the least upper bound.
   Subject level: 1011.

   (c) I have one subject at level 0110 and another subject at 0111. What is the most appropriate level for an object to be assigned so both subjects can append to the object? **0.25 Mark**
   ***No write down. The level of the object needs to dominate the levels of the subjects at levels 0110 and 0111.
   Object level: 0111. Note in particular that a level dominates itself.

   (d) I have three objects, one at 1000, one at 0100, and one at 0010. What is the most appropriate level for a subject to be assigned so all three objects can be read by the subject? **0.25 Mark**
   ***No read up. The level of the subject needs to dominate the levels of the objects at levels 1000 and 0100 and 0010.
   Subject level:1110.

   (e) Explain how the digits can be interpreted in a multilateral and multilevel sense. **0.5 Mark**
   **The first three digits correspond to categories. The last digit is like the sensitivity, e.g., secret vs top secret.

4. Assume that Alice has registered with the server Bob to use Lamport's one–time password scheme. Alice's password is `Alice1234567`, where you should replace the `1234567` with your own student

number. If $n = 10$ initially, what are the first two and the last one–time passwords transmitted by Alice? Use MD5 as the hash function. **0.5 Mark**

***$H^9(Alice1234567), H^8(Alice1234567)$ and the final password is $H^0(Alice1234567) = Alice1234567$.

5. Consider the BLP level relationship diagram in 862-A1-Q5.pdf, and the associated explanation of the notation, and answer the subsequent questions.

   (a) Does the diagram define a lattice? Justify your answer. **0.25 Mark**

   *** No because there is no greatest lower bound on levels F and K.

   (b) Assume that if the diagram didn't define a lattice you have fixed it so it does, without changing the relationships between the existing levels. Some of the domination relationships shown in the diagram are redundant. Identify two such lines and explain why they are unnecessary.

   *** In each case lines can be removed due to the transitive property of the domination relation. The line from K→C and the line from D→A and the line from G→J can each be removed.

   0.25 Mark