18/08/2016 CSCI862 Assignment 1 P1

Yixiang Fan
范翼翔
5083898

Part One : Short answer questions

1. The number of possible passwords:

$21 \times 5 \times 21 \times 10^3 \times 5^2 = 55125000$.

Entropy $= \log_2 55125000 = \frac{\log_{10}^{55125000}}{\log_{10}^{2}} \approx 25.7162$

When apply whirlpool hash function to get a 128 bit hex string, there will be at most 55125000 possible different output. But the whirlpool may incur collision, so the pratical different output may be less than 55125000. As a result, the entropy of the output is equal to or less than the entropy of passwords.

2. (1) Subjects: Alice; Bob; Chris; Dan

Objects: walls; fences; doors; Alice

Actions: climb; jump; push; open

(2)

Subject \ Object	walls	fences	doors	Alice
Alice	climb	jump		
Bob	push		push	
Chris	jump	push		push
Dan			open	jump

18/08/2016 CSCI862 Assignment 1 P2

Yixiang Fan
范翼翔
5083898

3. (a) They have a set $\{(a_1 a_2 a_3 a_4) | a_i \in (0,1)\}$ and a partial order like (0100) dom (0000). This order meets reflexive, antisymmetric and transitive relation. So they can regarded as lattices and they are same lattices.

(b) 1011

(c) 0111

(d) 1110

(e) Each digit can be interpreted as a privilege. If level X dominates level Y, then level X has all privileges that level Y has and has extra privileges. But if level X and level Y are connected by one line and level X dominates level Y, then level X only has one extra privilege compared with level Y. This complies with principle of least privilege and is also the partial order of this lattice.

4. 1st:e53999a51b1df69f10708334ea7503ff

2nd:2b846f93a9bb9044c2277ff2c92425eb

10th:Alice5083898

18/08/2016 CSCI862 Assignment 1 P3

Yixiang Fan
范翼翔
5083898

5. (a) The diagram doesn't define a good lattice. It contains a set $L \in \{A \cdots K\}$ and a partial order. But there are at least 2 redundent relationships in the diagram. In addition, it seems like an error that H dom G. Generally, if H dom G, H should be higher than G in the diagram. Besides, if H dom G, relationship between J and G is redundent as well. So although this diagram contains the essential components of a lattice, a set and a partial order, it is still not a well-formed lattice.

(b) 

and 

are redundent, because 

and 

. This property is called transivity.