A circular design with a lock on it

Description automatically generated

CSCI262 – Assignment 1

Spring 2024

Sami Sheikh | System Security | 22/08/2024

# Part 1: Short Answer Questions

1. Determine the entropy associated with the following method of generating a password.

*Choose, and place in this order, one lower case letter, following by one upper case letter, followed by two digits, followed by @, followed by two letters, each upper or lower case, and then followed by four symbols drawn from the set {$,7,3,v,w,J,z,T}. Finally, apply the hash function Tiger to give an output string in hex which will be used as a password.*

Assume random choices are made with equal likelihood of each symbol from the space being chosen from. So, for a random digit there are 10 possibilities, each chosen with probability 1/10.

## Answer 1

The entropy calculated for each case:

* One lowercase letter:
  + Since there are 26 possible lowercase letters
  + Entropy will be
* One uppercase letter:
  + Since there are 26 possible uppercase letters
  + Entropy will be
* Two digits:
  + Since each digit has 10 possible choices (from 0 to 9)
  + Entropy for each digit becomes =
  + Hence, for two digits: Entropy is =
* One ‘@’ symbol:
  + Since the @ symbol is a single and fixed choice, the entropy is nil
  + Entropy =
* Two letters (each either being uppercase or lowercase):
  + Each letter can be either lowercase or uppercase, meaning total entropy choices
  + Entropy for each letter becomes
  + Total entropy becomes:
* Four symbols from the set of *{$,7,3,v,w,J,z,T}:*
  + The set contains total of 8 symbols
  + Entropy for each symbol becomes
  + Entropy for 4 symbol becomes
* The hash function does not affect entropy as it just preserves it, unless it is salted.

Total Entropy :

1. For the following collection of statements, describe the sets of actions, objects, and subjects; and draw an access control matrix to represent the scenario.

* Alice can climb trees and eat apples.
* Bob can climb fences, eat apples, and wave flags.
* Trees can hurt apples.
* Carol can jump waves, eat apples, and wave flags.

## Answer 2

The set of subjects that can perform actions are:

1. Alice
2. Bob
3. Carol
4. Trees

The set of objects which are entities that actions can be performed on are:

1. Trees
2. Fences
3. Apples
4. Flags
5. Waves

The actions/operations that subjects can perform on objects are:

1. Climb
2. Eat
3. Wave
4. Jump
5. Hurt

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
|  | Trees | Fences | Apples | Flags | Waves |
| Alice | Climb |  | Eat |  |  |
| Bob |  | Climb | Eat | Wave |  |
| Carol |  |  | Eat | Wave | Jump |
| Trees |  |  | Hurt |  |  |

1. Assume an application requires access control policies based on the applicant’s age and the type of funding to be provided. Using an ABAC (attribute-based access control) approach, write policy rules for each of the following scenarios:
2. If the applicant’s age is more than 35, only “Research Grants (RG)” can be provided.
3. If the applicant’s age is less than or equal to 35, both “RG and Travel Grants (TG)” can be provided.

## Answer 3

Attribute-based access control systems make decisions based on the attributes of the subjects (users), objects (resources) and the environment (contextual information). As such, the attributes in this question would be the applicant’s age and the type of funding they are provided.

For policy (a), the condition is that the applicant’s age is more than 35, meaning they would only get access to Research Grants (RG)

ABAC Policy Rule:

For policy (b), the condition is that the applicant’s age is <= 35 year, hence they would get access to Research Grants (RG) and Travel Grants (TG)

ABAC Policy Rule: