

UNIVERSITY OF
WOLLONGONG



CSCI262 - SYSTEM SECURITY

Assignment 1: Part A

Harsha Vardhan Alagurajan
7768680

August 30, 2024

1.

To calculate the entropy associated with the password generation method, we consider the following components:

- One lowercase letter: 26 possibilities
- One uppercase letter: 26 possibilities
- Two digits: $10 \times 10 = 10^2$ possibilities
- Symbol @: 1 possibility
- Two letters (each can be upper or lower case): $52 \times 52 = 52^2$ possibilities
- Four symbols drawn from the set $\{\$, 7, 3, v, w, J, z, T\}$: 8^4 possibilities

The total entropy H is calculated as the sum of the logarithms (base 2) of the number of possible outcomes for each part:

$$H = \log_2(26) + \log_2(26) + 2\log_2(10) + \log_2(1) + 2\log_2(52) + 4\log_2(8)$$

Simplifying:

$$H = 2\log_2(26) + 2\log_2(10) + 2\log_2(52) + 4\log_2(8)$$

Substituting the values:

$$\log_2(26) \approx 4.7004, \quad \log_2(10) \approx 3.3219, \quad \log_2(52) \approx 5.7004, \quad \log_2(8) = 3$$

Thus, the total entropy H is:

$$H \approx 2(4.7004) + 2(3.3219) + 2(5.7004) + 4(3)$$

$$H \approx 9.4008 + 6.6438 + 11.4008 + 12$$

$$H \approx 39.4454 \text{ bits}$$

Therefore, the total entropy associated with this method of generating a password is approximately 39.45 bits.

2.

For the given collection of statements, we first identify the sets of subjects, objects, and actions:

- **Subjects:** Alice, Bob, Carol
- **Objects:** Trees, Apples, Fences, Waves, Flags
- **Actions:** Climb, Eat, Wave, Hurt, Jump

Access Control Matrix

The access control matrix representing the scenario is shown below:

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

3.

The following ABAC policy rules are defined based on the applicant's age and the type of funding:

- **Scenario (a):** If the applicant's age is more than 35, only "Research Grants (RG)" can be provided.

Policy Rule 1: $\text{can_access}(s, \text{RG}, e) \leftarrow (\text{Age}(s) > 35)$

- **Scenario (b):** If the applicant's age is less than or equal to 35, both "Research Grants (RG)" and "Travel Grants (TG)" can be provided.

Policy Rule 2: $\text{can_access}(s, \text{RG}, e) \leftarrow (\text{Age}(s) \leq 35)$

Policy Rule 3: $\text{can_access}(s, \text{TG}, e) \leftarrow (\text{Age}(s) \leq 35)$