**System Secutiry Assingment 1**

**Name: Jeslyn Ho Ka Yan**

**Sim id: 10241485**

**Part One: Short Answer Questions:**

**Question1**

**Password Structure:**

English alphabet consists of 26 letters. There are 5 Vowels

Δ is a consonant (C): 26−5=21choices

Φ is Vowel: 5 choices

**Each Segment**

Since each segment is Δ Φ Δ (consonant, vowel, consonant),

21 × 5 × 21 =2205

**Total Number of Password**  
Since each password consist of two segment

2205 × 2205 =4860205

As a result, the generator has the capacity to produce 4,860,205 different passwords.

**Question2**

Alice’s pwd: Alice1234567

N =5

|  |  |  |
| --- | --- | --- |
| **Challenge (n-c)** | **Counter (c)** | **Respond𝐻𝑛−𝑐 (𝑆) = 𝑝𝑤𝑛−𝑖** |
| 4 | 1 | 𝐻4 (𝑆 )= 𝑝𝑤4 |
| 3 | 2 | 𝐻3(𝑆 )= 𝑝𝑤3 |
| 2 | 3 | 𝐻2 (𝑆 )= 𝑝𝑤2 |
| 1 | 4 | 𝐻1 (𝑆 )= 𝑝𝑤1 |
| 0 | 5 |  |

**The first three one-time passwords (OTPs) will be:**

* OTP 1: H4(P)
* OTP 2: H3(P)
* OTP 3: H2(P)

**The first three one-time passwords (OTPs) transmitted by Alice are:**

1. **OTP 1**: H4(P)= 7620a7f4c73177c31620cdfe3eded58e
2. **OTP 2**: H3(P)= f3ad0072adf2803a4dd7afd4ceec6d7d
3. **OTP 3**: H2(P)= 58d412d46635f99d5a65fc9b9d19b98f

**Question3**

**a. Does a lattice get defined in the diagram?**

**A lattice in the context of BLP must satisfy two conditions:**

For each pair of components (levels) in the hierarchy, there needs to have a

1. **Least Upper Bound (LUB),** requires that there be a distinct, least level that is bigger than or equal to each pair of levels
2. **Greatest Lower Bound (GLB),** or meet: There must be a distinct, greatest level that is less than or equal to each of each pair of levels.

Looking at the diagram, we can see that the structure permits some elements to connect via more than one way, but not every node has distinct greatest lower bounds and least upper bounds for every pair that could exist. For example, node T is connected to S (directly) and P (indirectly through Y).

This structure **does not constitute a lattice** because of these ambiguities in the unique least upper bounds and largest lower bounds for specific pairs.

**b. List two such relationships and provide an explanation for their needlessness.**

1. **P → S relationship is redundant:**

If P→Q and Q→S are maintained, then P→S is implied by transitivity. Thus, the direct relationship from P→S would be redundant.

1. **P → T relationship is redundant:**

if P→Y and Y→T exist, then P→T can be considered redundant by transitivity.

Since other paths in the diagram can be used to deduce these links, they are not required. Lessening these repetitions could make the diagram simpler and guarantee that, with additional modifications, it defines the correct lattice structure.

**Question4**

**a. subjects, objects, and actions**

Subject : Alexis, Boris, Catherine, Duggy

Object: Balls, Sticks, Boris

Actions: Kick, Throw, catch, snap, roll, chew, fetch

**b. Access Control Matrix**

|  |  |  |  |
| --- | --- | --- | --- |
|  | **Balls** | **Sticks** | **Boris** |
| **Alexis** | Kick | Throw | - |
| **Boris** | Catch, Kick | Throw | - |
| **Catherine** | Roll | Snap | - |
| **Duggy** | Chew | Fetch | Chew |

**c. access control lists**

Balls: (Alexis, kick), (Boris, catch,kick), (Catherine, roll), (Duggy, chew)

Sticks: (Alexis,throw), (Boris, throw), (Catherine, snap), (Duggy, fetch)

Boris: (Duggy, chew)

**d. capability lists**

Alexis: (Balls, Kick), (Sticks, Throw)

Boris: (Balls, Catch, Kick), (Sticks, Throw)

Catherine: (Balls, Roll), (Sticks, Snap)

Duggy: (Balls, Chew), (Sticks, Fetch), (Boris, Chew)

**Part Two: Two factor Authentication**

Output

1st terminal for connect.py

[10/30/24]seed@VM:~$ cd /home/seed/mySpace/A1

[10/30/24]seed@VM:~/.../A1$ python3 connect.py newjeans new

Enter new password: bunny123!

Confirm new password: bunny123!

User registered successfully.

[10/30/24]seed@VM:~/.../A1$ python3 connect.py newjeans bunny123! 803005

Invalid or expired PIN.

[10/30/24]seed@VM:~/.../A1$ python3 connect.py newjeans bunny123! 751292

Invalid or expired PIN.

[10/30/24]seed@VM:~/.../A1$ python3 connect.py newjeans bunny123! 274360

User authenticated successfully.

PIN is valid and used successfully.

[10/30/24]seed@VM:~/.../A1$ python3 connect.py newjeans bunny123! 274360

Invalid or expired PIN.

[10/30/24]seed@VM:~/.../A1$

A screen shot of a computer code

Description automatically generated

Output

2st terminal for device.py

[10/30/24]seed@VM:~/.../A1$ python3 device.py newjeans bunny123!

Starting device...

Device: 803005

Device: 751292

Device: 274360

Device: 910813

^C

Device stopped by user.

[10/30/24][seed@VM:~/.../A1$](mailto:seed@VM:~/.../A1$)

A screen shot of a computer

Description automatically generated