جامعة بيرزيت

BIRZEIT UNIVERSITY

Name : Jumana Abu Murra Wednesday

ID : 1220594 21/12/2022

Assignment #1

Question 1:

Explain the difference between authentication and identification.

Authentication	Identification
➢ By authentication we mean verifying a claimed identity ➢ Identity is provided ➢ Is he really who he claims to be? ➢ One-to-one verification	➢ By identification we mean establishing an identity ➢ No identity is provided ➢ Who is he? ➢ One-to-many

Question 2:

What 7 characteristics should a biometric feature have? Explain them briefly.

Universality	>Each person should have the characteristic >Failure to Enroll Rate (FER)
Distinctiveness	> Different persons should have different biometric properties > False Match Rate (FMR)
Permanence	> The characteristic should be sufficiently invariant over a period of time >False Non-Match Rate (FNMR)

Collectability	> The biometric property should be easy to collect (electronically) and to quantify
Performance	>This refers to the achievable recognition accuracy and speed >False Non Match Rate (FNMR) > Failure to Capture Rate (FCR)
Acceptability	>To which extent are people willing to accept the use of a specific biometric
Circumvention	> Reflects how easy it is to fool the system > False Match Rate (FMR)

Question 3:

(a) Consider the voice recognition system. Which is the best for accuracy: standard or nonstandard environment? Why?

Non-standard because this System in a dynamic environment e.g. background noise for voice recognition and voice is dynamic environment based system

(b) Consider the on-line signature recognition system. Is the system covert or overt? Why?

overt because User is aware that the biometric feature is being measured e.g. finger on fingerprint reader and on-line signature is biometric feature is being measured

(c) Consider the retinal recognition system, which is non-attended and non-habituated. What kind of problems will most probably occur and what kind of errors can these problems lead to?

The problems:

1) When changing the features of the retina, such as wearing contact lenses.

2) Identification is made from a short distance.

3) This feature dose not work for blind people

4) When the eye is injured

5) when person dies, the fingerprint does not recognize the retine.

Errors:

1) FNMR 2) FCR 3) FER

Question 4:

FMR A hand geometry recognition system is tested and the total comparison scores are listed on Table 1. A1, B1, C1, D1 and E1 are enrolled persons and A2, B2, C2, D2 and E2 are test samples from the same persons.

Users	A2	B2	C2	D2	E2
A1	0.12	3.74	1.52	3.31	4.31
B1	3.81	0.08	0.97	3.00	3.85
C1	1.53	1.21	0.98	1.22	2.21
D1	3.24	3.00	0.99	0.25	3.45
E1	4.30	3.65	2.45	3.46	0.17

Table 1: The comparison scores of a hand geometry recognition system

(a) If the threshold value is set to 1,00, what is FMR?

FMR= 2/20

(b) If FMR is wanted to be zero, what is the threshold value and FNMR then?

FMR = /20

0 = X/20

X=0

the probability is zero

according to the condition

d<t

the lowest value for d=0.97

out of 120 possibilities

t=the smallest value because

it has zero probability

any value less than 0.97

d< *t* FMR=0/20

d> t FNMR=1/5

Question 5:

(a) How many 6 character passwords are there which have exactly one K?

1	2	3	4	5	6
K					

K you put it any position

$6*93^5 = 4.174130216*10^{10}$

(b) What is the number of 6 character passwords containing the word "ape"?

ape hold 3 position and has 4 possibilities

a	P	e			
	a	p	e		
		a	p	e	
			a	p	e

$4*94^3$ = 3.322.336

(c) How many 6 character passwords are there which have at least 4 numbers?

(333333)	true	true	true	true
(AaAaAa)	false			
(aaaaaa)	false			
(@@@@@@)	false			

The trick = All – wrong ones + those subtracted twice
$=94^6 - 54^6$+0(because there's not subtracted twice)
=665074869760

Question 6:

Deploy the most suitable concept that represents each of the following statements:

(a) A cybersecurity administrator in a particular organization was able to detect a suspicious behavior in the database server, and then he decided to verify the log files of that server in order to figure out who did this suspicious action.

accounting

(b) An external user was able to conduct a scanning process on the system of an organization and specifying the weaknesses in that system, and then he sent an email to the organization informing them about their weaknesses.

White-hat hacker

(c) A fake email was sent to an employee in a company pretending to be sent from the network manager that asks employees for verifying their accounts by writing sensitive and secure information, such as password, user name, and ID number.

phishing

(d) An attacker was able to control 1000 computer machines in different countries by using malicious software, and then he decided to target a website of University, which leads to the inability of students from accessing their accounts on the university portal.

DDOS

(e) An attacker was able to reveal the secret cryptography algorithm that used by two users in their communication, by knowing the plaintext and its corresponding encrypted text of multiple messages.

Known-plaintext attack

Question 7:

Write a complete scenario using the Ritaj system of Birzeit University as an example that shows clearly the following cybersecurity concepts:

I. Authorization

II. Authentication

III. Availability

Ritaj is the name of the student management system at Birzeit University. it is used by student, teachers, and administrators to access important information and resources related to their studies classes ,and assignments.

One day, a hacker managed to gain unauthorized access to the Ritaj system and started tampering with the date stored in it. The hacker changed the grades of some students, deleted important assignments and course materials, and disrupted the availability of the system for the legitimate users.

The university administration quickly realized the situation and took action to prevent further damage, they contacted their cybersecurity team and implemented additional security measures to block the unauthorized access and restore the availability of the Ritaj system.

The cybersecurity team implemented a system of authorization, where only authorized users with valid credentials were allowed to access the Ritaj system, they also implemented an authentication system, where the identity of each user was verified before they were granted access.

With these measures in place, the Ritaj system was restored to its normal availability and the legitimate users were able to access the information and resources they needed. The university administration also launched an investigation to identify the hacker and prevent similar attacks in the future.

The incident at Birzeit University highlighted the importance of strong cybersecurity measures, including authorization and authentication, to protect the availability of critical systems and prevent unauthorized access.

Question 8:

Dictionary attack and brute force attack are two attacks that are used to penetrate the authentication mechanism of a system by revealing the proper password of that system, list at least three practices/strategies in order to strengthen a system against such these two attacks.

1) Use strong password
2) Change your passwords regularly
3) Don’t use the same password for all account