Homework 5 Quiz

Due Feb 15 at 10am **Points** 34 **Questions** 22
Available Feb 9 at 12am - Feb 15 at 10am 6 days **Time Limit** None

Instructions

Authentication

Before starting this online assignment:

- Read Chapter 3
- Review the **Data Security** slides on Authentication
- Chapter 3 Review Problems
  - Problem 3.1
  - Problem 3.8

Attempt History

	Attempt	Time	Score
LATEST	Attempt 1	3,023 minutes	29.6 out of 34

Correct answers will be available on Feb 16 at 12am.

Score for this quiz: **29.6** out of 34
Submitted Feb 14 at 4:34pm
This attempt took 3,023 minutes.

Question 1 — 1 / 1 pts

User authentication is a procedure that allows communicating parties to verify that the contents of a received message have not been altered and that the source is authentic.

True

- False

Question 2

1 / 1 pts

A _____ is a separate file from the user IDs where hashed passwords are kept

- shadow password file
- hidden password file
- secure password file
- secret password file

Question 3

1 / 1 pts

The means of authenticating a users identify are:

- Something you know and Someone Who Can Vouch for You
- Something you and Something you have
- Something you have, Something you do, and Something you are
- Something you know, Something you can prove, and Something You own

Question 4

1 / 1 pts

Objects that a user possesses for the purpose of user authentication are called

tokens

Question 5

1 / 1 pts

User authentication is the basis for most types of access control and for user accountability.

- True
- False

Question 6

1 / 1 pts

Recognition by fingerprint, retina, and face are examples of

- dynamic biometrics
- token authentication
- face recognition
- static biometrics

Question 7

1 / 1 pts

Enrollment creates an association between a user and the user's biometric characteristics.

- True
- False

Question 8

1 / 1 pts

The SSH login protocol sends passwords in clear text and anyone who can observe the messages can learn the password.

- True
- False

Question 9

1 / 1 pts

Unix systems store passwords in the clear on the server and provide security by ensuring only the root user has access to the file.

- ○ True
- ◉ False

Question 10

1 / 1 pts

HTTP sends passwords in clear text and anyone who can observe the messages can learn the password.

- ◉ True
- ○ False

Question 11

2 / 2 pts

A new operating system uses passwords that consist of three characters. Each character must be a digit between 0 and 9. For example, three distinct possible passwords are 123, 416, and 999. The system uses ***32 bit salt values***. The system also allows one login attempt every second and never locks out users regardless of how many failed attempts occur.

If an adversary has obtained a copy of the password file and conducts an offline brute force attack against Bob's password by trying every password combination until the adversary obtains Bob's password. The adversary is

only interested in obtaining Bob's password and gets no benefit from obtaining any other user's password. Increasing the salt value from 32 to 64 bits will make it more difficult for the adversary's attack to succeed.

- True
- False

Question 12

2 / 2 pts

Assume passwords are selected from four character combinations of 26 alphabetic characters. Assume an adversary is able to attempt passwords at a rate of 1 per second. Assuming feedback to the adversary flagging an error as each incorrect character is entered, what is the expected time to discover the correct password? (Enter the number of seconds)

52

Question 13

2 / 2 pts

Assume passwords are selected from four character combinations of 26 alphabetic characters. Assume an adversary is able to attempt passwords at a rate of 1 per second. Assuming no feedback to the adversary until each attempt is completed, what is the expected time to discover the correct password? (Enter the number of seconds)

228488

Incorrect

Question 14

0 / 2 pts

A new operating system uses passwords that consist of three characters. Each character must be a digit between 0 and 9. For example, three distinct possible passwords are 123, 416, and 999. The system uses ***32 bit salt values***. The system also allows one login attempt every second and never locks out users regardless of how many failed attempts occur.

An adversary has learned there is an account with username Bob and the adversary can attempt to login as Bob. If the adversary uses a brute force attack, what is the expected amount of time to crack Bob's password? (enter a decimal number of seconds)

First calculate the total number of passwords. The expected number of tries the adversary must make is half the number of passwords. The adversary simply enters the possible password and the login process verifies it is correct. Each try takes 1 second.

Question 15

2 / 2 pts

Assume source elements of length 6 are mapped in some uniform fashion into target elements of length 3. Each digit can take on one of 9 possible values. Thus the number of source elements is 531,441 and the number of target elements is 729. A particular source element x is mapped to a target element y.

If the adversary is given element y, what is the probability that a different source element z (z not equal to x) that produces the target value y can be produced by the adversary in one try? (enter you answer as an exact decimal number like 0.XXXXXX...XXX)

0.00136986043

Question 16

2 / 2 pts

A new operating system uses passwords that consist of three characters. Each character must be a digit between 0 and 9. For example, three distinct possible passwords are 123, 416, and 999. The system uses ***32 bit salt values***. The system also allows one login attempt every second and never locks out users regardless of how many failed attempts occur.

If an adversary has obtained a copy of the password file and conducts an offline brute force attack by trying every password combination until the adversary obtains username and password combination. The use of a 32 bit salt value

- improves security because the adversary must guess both the username and the salt value for each user.
- Improves security because the use of salt value prevents the adversary from conducting a cryptoanalytic attack against the password hash
- improves security because the adversary has to consider each user and password individually
- does not improve security because the adversary has obtained the password file that lists the salt value.

Incorrect

Question 17

0 / 2 pts

A new operating system uses passwords that consist of three characters. Each character must be a digit between 0 and 9. For example, three distinct possible passwords are 123, 416, and 999. The system uses ***32 bit salt values***. The system also allows one login attempt every second and never locks out users regardless of how many failed attempts occur.

If an adversary uses a brute force by repeatedly trying to login as Bob, increasing the salt value from 32 to 64 bits will make it more difficult for the adversary's attack to succeed.

- (●) True
- ( ) False

The adversary simply enters the possible password and the login process verifies it is correct. Each attempt takes 1 second and the length of the salt value has no impact.

Question 18

2 / 2 pts

Assume source elements of length 6 are mapped in some uniform fashion into target elements of length 3. Each digit can take on one of 9 possible values. Thus the number of source elements is 531,441 and the number of target elements is 729. A particular source element x is mapped to a target element y.

If the adversary is given element y, what is the probability the correct source element can be selected by the adversary in one try? (enter you answer as an exact decimal number like 0.XXXXXX...XXX)

0.00000188167

Question 19

2 / 2 pts

A new operating system uses passwords that consist of three characters. Each character must be a digit between 0 and 9. For example, three distinct possible passwords are 123, 416, and 999. The system does not use any salt values. The system also allows one login attempt every second and never locks out users regardless of how many failed attempts occur.

An adversary has learned there is an account with username Bob and the adversary can attempt to login as Bob. If the adversary uses a brute force attack, what is the expected amount of time to crack Bob's password? (enter a decimal number of seconds)

500

Partial

Question 20

1.6 / 2 pts

Bloom Filters: Students at Some State University (SSU) select

very bad passwords. The system administrator decided to use a *Bloom Filter* to prevent students from using the passwords "cat, dog, fish, and bear". The Bloom Filter uses 3 hash functions (H1, H2, H3) and 10 bits in the hash table. When the hash functions are applied to the prohibited passwords, the results are:

H1(cat) = 8 H2(cat) = 1 H3(cat) = 2

H1(dog) = 1 H2(dog) = 9 H3(dog) = 1

H1(fish) = 2 H2(fish) = 8 H3(fish) = 2

H1(bear) = 2 H2(bear) = 4 H3(bear) = 1

Enter the resulting Bloom Filter by marking each bit as either 0 or 1.

Bit 0	Bit 1	Bit 2	Bit 3
0	`1	1	0

Answer 1:

0

Answer 2:

`1

Answer 3:

1

Answer 4:

0

Answer 5:

1

Answer 6:

0

Answer 7:

0

Answer 8:

0

Answer 9:

1

Answer 10:

0

Question 21

2 / 2 pts

Bloom Filters: Students at Some State University (SSU) select very bad passwords. The system administrator decided to use a *Bloom Filter* to prevent students from using the passwords "cat, dog, fish, and bear". The Bloom Filter uses 3 hash functions (H1, H2, H3) and 10 bits in the hash table. When the hash functions are applied to the prohibited passwords, the results are:

H1(cat) = 8 H2(cat) = 1 H3(cat) = 2

H1(dog) = 1 H2(dog) = 9 H3(dog) = 1

H1(fish) = 2 H2(fish) = 8 H3(fish) = 2

H1(bear) = 2 H2(bear) = 4 H3(bear) = 1

A student selects the password "mouse". Note this not a prohibited password. Before the password is accepted, it will be checked against the Bloom Filter. Hash functions H1 and H2 are applied to "mouse" and the results are:

H1(mouse) = 4 H2(mouse) = 8

List one value for H3(mouse) that would cause the "mouse" to be rejected as a password or enter -1 if there is no such value

1

Question 22

2 / 2 pts

Bloom Filters: Students at Some State University (SSU) select very bad passwords. The system administrator decided to use a *Bloom Filter* to prevent students from using the passwords "cat, dog, fish, and bear". The Bloom Filter uses 3 hash functions (H1, H2, H3) and 10 bits in the hash table. When the hash functions are applied to the prohibited passwords, the results are:

H1(cat) = 8 H2(cat) = 1 H3(cat) = 2

H1(dog) = 1 H2(dog) = 9 H3(dog) = 1

H1(fish) = 2 H2(fish) = 8 H3(fish) = 2

H1(bear) = 2 H2(bear) = 4 H3(bear) = 1

A student selects the password "mouse". Note this not a prohibited password. Before the password is accepted, it will be checked against the Bloom Filter. Hash functions H1 and H2 are applied to "mouse" and the results are:

H1(mouse) = 4 H2(mouse) = 8

List one value for H3(mouse) that would cause the "mouse" to be accepted as a password or enter -1 if there is no such value

6

Quiz Score: **29.6** out of 34