CSCI 3403 **Name:** _____
Spring 2020
Midterm Exam
03/05/2020
Time Limit: 75 Minutes

This exam contains 10 pages (including this cover page) and 34 questions.
Total of points is 100.

---

1. (1 point) The correct answer is A. Good luck!
    A. **The correct answer**
    B. An incorrect answer
    C. Another incorrect answer
    D. The last incorrect answer

2. (2 points) Which of the following is the best example of Open Design?
    A. Two-Factor Authentication
    B. **Using a well-known cryptographic algorithm**
    C. Separating roles for IT and HR
    D. A safe locks when the power goes out

3. (2 points) Which of the following is the best example of Defense in Depth?
    A. **Two-Factor Authentication**
    B. Using a well-known cryptographic algorithm
    C. Separating roles for IT and HR
    D. A safe locks when the power goes out

4. (2 points) Which of the following is the best example of Fail-safe Defaults?
    A. Two-Factor Authentication
    B. Using a well-known cryptographic algorithm
    C. Separating roles for IT and HR
    D. **A safe locks when the power goes out**

5. (2 points) Our security system is out of date! Consider a scenario where hackers want to break into our network and steal our MySQL database of credit card information. Which of the following best describes the risk in this situation?
    A. Attackers want to break in and steal our credit card info
    B. **There is a high probability of having credit cards breached**
    C. The attackers
    D. The out of date MySQL and PHP versions

6. (2 points) Consider the following BLP scenario: Alice has clearance U and a document has clearance $(C, \{A\})$. Alice can...
    A. Neither read nor write
    B. Read, but not write
    C. **Write, but not read**
    D. Both read and write

7. (2 points) Consider the following BLP scenario: Bob has clearance *(S, {A})* and a document has clearance *(S, {B})*. Bob can...

   A. **Neither read nor write**

   B. Read, but not write

   C. Write, but not read

   D. Both read and write

8. (2 points) Consider the following BLP scenario: Cathy has clearance *(TS, {A, B})* and a document has clearance *(S, {B})*. Cathy can...

   A. Neither read nor write

   B. **Read, but not write**

   C. Write, but not read

   D. Both read and write

9. (2 points) Which of the following is NOT a legitimate way of providing message authentication?

   A. MAC

   B. Digital signature

   C. **Digital envelope**

10. (2 points) Alice wants to send a message to Bob and guarantee the *integrity* of the message. Given a secure hash function H, a message M, and a shared secret K, which of the following should Alice send? (+ is concatenation)

    A. H(M + K)

    B. **M + H(M + K)**

    C. M + H(K)

    D. H(M) + H(K)

11. (2 points) Which of the following refers to an unauthorized way of gaining access to a program, online service, or an entire computer system?

    A. Logic bomb

    B. Trojan horse

    C. Rootkit

    D. **Backdoor**

12. (2 points) A collection of hacker tools used by an attacker after gaining administrator-level access on a computer is called a...

    A. Logic bomb

    B. Trojan horse

    C. **Rootkit**

    D. Backdoor

13. (2 points) Which symmetric encryption mode offers message integrity?

    A. ECB
    B. CBC
    C. CFB
    D. OFB
    E. CTR
    F. **GCM**

14. (2 points) (True/False) It is possible to delete an item from a Bloom Filter without rebuilding the filter or compromising the integrity of the check.

    A. True
    B. **False**

15. (2 points) (True/False) An ideal cryptographic hashing algorithm will have no collisions.

    A. True
    B. **False**

16. (2 points) (True/False) Viruses need a host to attach to while worms do not

    A. **True**
    B. False

17. (2 points) (True/False) An amplification attack is a variant of a reflection attack

    A. **True**
    B. False

18. (2 points) (True/False) In a successful replay attack, the adversary must necessarily be able to decrypt the messages

    A. True
    B. **False**

19. (2 points) (True/False) The setuid bit affects who can run a program in Linux

    A. True
    B. **False**

20. (2 points) (True/False) Kerberos uses tickets to authenticate its users rather than sending passwords over the network.

    A. **True**
    B. False

21. (2 points) We have a system that uses 4 character-long passwords with only lower-case characters and a 32-bit salt. The adversary performs an **online** attack against Bob. The adversary can guess one password per second, and the system has no lockouts. On average, how long would we expect the adversary to take in order to crack Bob's password?

A. 0-10s
B. 10-100s
C. 100-1,000s
D. 1,000-10,000s
E. 10,000-100,000s
F. **100,000s+**

22. (3 points) We have a system that uses 4 character-long passwords with only lower-case characters and no salts. The adversary performs an **offline** attack against Bob. The adversary can hash and compare one hundred passwords per second. On average, how long would we expect the adversary to take in order to crack Bob's password?

A. 0-10s
B. 10-100s
C. 100-1,000s
D. **1,000-10,000s**
E. 10,000-100,000s
F. 100,000s+

23. (3 points) We have a system that uses 4 character-long passwords with only lower-case characters and a 32-bit salt. The adversary performs an **offline** attack against Bob. The adversary can hash and compare one hundred passwords per second. On average, how long would we expect the adversary to take in order to crack Bob's password?

A. 0-10s
B. 10-100s
C. 100-1,000s
D. **1,000-10,000s**
E. 10,000-100,000s
F. 100,000s+

24. (3 points) We have 3 jobs. Each job has 9, 5, and 4 users, respectively, as well as 4, 5, and 3 permissions required for each role, respectively. In a traditional RBAC scheme, how many relationships between users and permissions must be defined?

A. 18
B. **30**
C. 73
D. 240

25. (3 points) In order to keep our sensitive data safe on our company laptop, we decide to encrypt the hard drive to keep prying eyes off. The user should be able to enter a password to decrypt their data when the computer boots. Which of the following encryption algorithms is best suited for our task?

A. **AES**
B. RSA
C. SHA-256
D. None of the following would work

26. (3 points) Which of the following is an example of a PHP superglobal?

A. **$_SESSION**
B. $myvar
C. global $x
D. None of the above

27. (3 points) We roll three dice and observe the results. In what range is the probability that all three dice show distinct values?

A. 0-0.15
B. 0.15-0.3
C. 0.3-0.4
D. 0.4-0.5
E. **0.5-0.6**
F. 0.6-0.7
G. 0.7-0.85
H. 0.85-1

28. (4 points) On our PHP server, we have a very flat authentication system (either you're authenticated or you're not). We have a function that gets called to authenticate a user. Assume that $*conn* holds a legitimate connection with a MySQL server.

```
function db_authenticateUser() {
    global $conn;
    $user = $_POST['user'];
    $pass = $_POST['pass'];
    $q = "SELECT user_name, password FROM `users` WHERE".
             " user_name='$user' AND password='$pass'";
    $r = mysqli_query($conn, $q);
    if(!empty(db_parseResult($r)))
        return true;
    else
        return false;
}
```

Which of the following best describes the biggest problem with the function shown above?

A. **Vulnerable to SQL injection**
B. Syntax errors
C. Logically doesn't work
D. Relies on client-side validation

29. (4 points) Which set of algorithms is considered secure for modern use?

A. 3DES, MD5, RSA
B. AES, SHA-1, RSA
C. **AES, SHA-3, RSA**
D. AES, MD5, ECC
E. 3DES, SHA-3, RSA
F. DES, SHA-256, ECC

30. (5 points) Consider a typical PKI scenario using TLS v1.2. How does the server most commonly authenticate the user?

With a username and password.

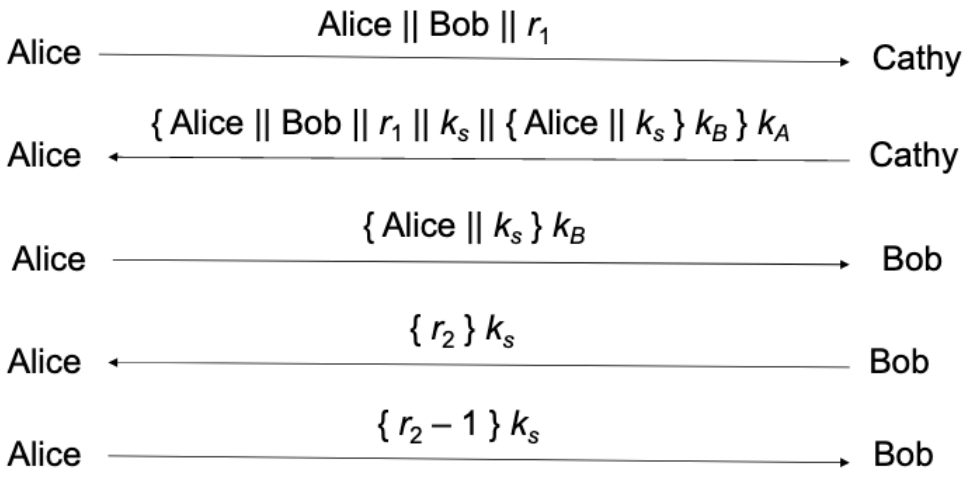
31. (5 points) Give the four ways of authenticating a user (no explanation needed).

Something the user has, something the user knows, something the user is, and something the user does

32. (5 points) What is the difference between authentication and authorization?

Authentication is verifying who the user is, and authorization is verifying what the user can do. Authentication must happen before authorization is possible.

33. (8 points) Consider the replay attack scenario shown below. It is well-known that Bob uses the current time with relatively low precision to seed his random numbers (a huge no-no!!). As a result, Eve finds that she can predict the random number Bob sends over with a 10% accuracy, though the random numbers are never used more than once. Assuming Eve never learns k_s, k_B, or k_A, is this scheme safe from replay attacks? Explain why or why not.



The schema is indeed safe from replay attacks. In this scenario, case 2 from the slides, Eve must learn k_s in order to perform a replay attack. Although Eve may in some cases know r_2, simply knowing r_2 is not enough to send it back in its encrypted form. As long as Bob never sends the same random number more than once, Eve will never have an encrypted version of the challenge to send back.

34. (10 points) The course staff for Intro to Cybersecurity got together and decided to make a revised version of the Diffie-Hellman Key Exchange Algorithm as follows. First, they generate a public prime number p and base $g < p$. Then, Party 1 and Party 2 generates their secrets, $x_1 < p-1$ and $x_2 < p-1$, respectively (the same as the old Diffie-Hellman thus far). Then, they calculate

$$y_1 = g^{x_1} \qquad y_2 = g^{x_2}$$

They exchange y_1 and y_2 over an insecure channel. Then they attempt to calculate their shared key z with

$$z = y_2^{x_1} \qquad z = y_1^{x_2}$$

(a) (5 points) Does the algorithm still result in the successful distribution of keys? Assume sufficiently large data structures for storing the numbers.

Yes, the new algorithm results in a successful key exchange. We can see that $y_1 = g^{x_1}$ and $y_2 = g^{x_2}$, then y_1 and y_2 are sent over the insecure channel. Then the z keys are calculated: $z_1 = {y_2}^{x_1} = (g^{x_2})^{x_1} = g^{x_2 x_1}$ and $z_2 = y_1^{x_2} = (g^{x_1})^{x_2} = g^{x_1 x_2}$. Because $z_1 = g^{x_2 x_1} = g^{x_1 x_2} = z_2$, that means that $z_1 = z_2 = z$, which means there was a successful exchange of keys.

(b) (5 points) Does the algorithm have any new security flaws? If so, describe them. If not, explain why the change is equally secure.

Yes, the algorithm has a new security flaw, in addition to the MitM flaw found in the original. y_1 and y_2 are sent over an insecure channel, and g is public. That means that the attack knows that $y_1 = g^{x_1}$. Since they know y_1 and g, then can easily calculate $\log_g(y_1) = \log_g(g^{x_1}) = x_1 \log_g(g) = x_1$, and they can do the same thing to find x_2. Once they have x_1 or x_2 they can easily compute the key z. This computation is extremely easy to perform, and in the regular Diffie-Hellman key exchange, this was made impossible with the modular arithmetic.

This page is intentionally left blank