Name

CWID

Exam

CS458 - Spring 2021 - Final Exam

Wednesday, May 12th, 2021
2:00 pm - 4:00 pm

Please leave this empty!

1.1 | 1.2 | 1.3 | 1.4 | 1.5 | Sum

Instructions

- **You have to hand in the exam via course blackboard**
- **This is an individual and not a group assignment. Fraud will result in 0 points**

BY SUBMITTING THIS EXAM THROUGH THE ONLINE SYSTEM, I AFFIRM ON MY HONOR THAT I AM AWARE OF THE STUDENT DISCIPLINARY CODE, AND (I) HAVE NOT GIVEN NOR RECEIVED ANY UNAUTHORIZED AID TO/FROM ANY PERSON OR PERSONS, AND (II) HAVE NOT USED ANY UNAUTHORIZED MATERIALS IN COMPLETING MY ANSWERS TO THIS TAKE-HOME EXAMINATION.

Question 1.1 True or False (20 Points)

1. (**1 pts.**) [True/False] Triple DES (3DES) is more secure than DES, but is slower.
2. (**1 pts.**) [True/False] Diffie-Hellman key exchange is an asymmetric scheme that can be used for encryption and signatures, but is not as efficient as RSA.
3. (**1 pts.**) [True/False] RBAC supports the principles of least privilege and separation of duty.
4. (**1 pts.**) [True/False] Symmetric key crypto can be used to achieve integrity, but not non-repudiation.
5. (**1 pts.**) [True/False] Hash functions can be used for intrusion and virus detections.
6. (**1 pts.**) [True/False] For any cipher, double encryption does not result in much increased security due to the meet-in-the-middle attack.
7. (**1 pts.**) [True/False] A weak hash function is sufficient to protect against an attack in which one party generates a message for another party to sign.
8. (**1 pts.**) [True/False] A public-key certificate scheme alone does not provide the necessary security to authenticate the public key.
9. (**1 pts.**) [True/False] In a traffic analysis attack, a malicious user observes patterns of communications, without having to read the message contents.
10. (**1 pts.**) [True/False] In `Mandatory Access Control`, resource owners can override system policy and allow other users access to his resources when the system forbids it.
11. (**1 pts.**) [True/False] In confusion, the statistical structure of the plaintext is dissipated into long-range statistics of the ciphertext. This is achieved by having each plaintext digit affect the value of many ciphertext digits, which is equivalent to saying that each ciphertext digit is affected by many plaintext digits.
12. (**1 pts.**) [True/False] Message authentication protects two parties who exchange messages from any third party, however, it does not protect the two parties against each other.
13. (**1 pts.**) [True/False] `X.509` defines the format for private-key certificates.
14. (**1 pts.**) [True/False] Least privilege means that a user executing a command should not have more privilege than needed for that command.
15. (**1 pts.**) [True/False] Access control is a security service that controls who can have access to a resource
16. (**1 pts.**) [True/False] In a replay attack, a malicious user sends an identical copy of a previous message they have intercepted.
17. (**1 pts.**) [True/False] A random number would be a good choice for a nonce.
18. (**1 pts.**) [True/False] Although public announcement of public keys is convenient, anyone can forge a public announcement.
19. (**1 pts.**) [True/False] The digital signature function does not include the authentication function
20. (**1 pts.**) [True/False] Once the server verifies that the user ID in the ticket is the same as the unencrypted user ID in the message it considers the user authenticated and grants the requested service

Question 1.2 (36 Points)

Circle the right answer(s):

1. (**2 pts.**) `SHA-1` produces a hash value of
   (a) `160 bits`
   (b) `224` bits
   (c) `256` bits
   (d) `512` bits
2. (**2 pts.**) The `*-property`, as shown in the `BLP model`, requires that there be:
   (a) no reads "up"
   (b) no reads "down"
   (c) no writes "up"
   (d) no writes "down"
3. (**2 pts.**) Which of the following statements is NOT true about Role-Based Access Control (RBAC)?
   (a) A user can be assigned one or more roles
   (b) A session can have one or more users
   (c) A session can have one or more roles
   (d) A role can be assigned to one or more users
4. (**2 pts.**) `AES` is a
   (a) block cipher
   (b) stream cipher
   (c) one-time pad
5. (**2 pts.**) ..... 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.
   (a) Verification
   (b) User authentication
   (c) Message authentication
   (d) Identification
6. (**2 pts.**) Which of these cryptographic attacks models is the strongest?
   (a) Ciphertext only
   (b) Chosen plaintext
   (c) Known plaintext
7. (**2 pts.**) What is/are essential properties of a one-time pad? (circle all that apply)
   (a) key length equal to plaintext length
   (b) key must be chosen randomly
   (c) keys can be reused
   (d) A & B
   (e) All of the above

8. (**2 pts.**) Each individual access control list (ACL) represents:

   (a) A row of the Access Control Matrix

   (b) A column of the Access Control Matrix

9. (**2 pts.**) Imagine a password system whose passwords require exactly 8 characters, from an alphabet of 32 characters. The system uses 4 bits of salt. The attacker acquires a copy of the encrypted passwords on the computer (but not the salt), there are 64 of them. The attacker knows the function used to encrypt passwords, and mounts a brute force attack generating legal passwords at random trying to find one for which there is a match in the password file.

   How many passwords must be randomly generated (assuming no memory is kept of passwords already tested) before finding a match? (circle only one)

   - 2^{32}
   - 2^{34}
   - 2^{36}
   - 2^{38}
   - None of the above

10. (**2 pts.**) To encrypt a series of plaintext blocks $p_1, p_2, \ldots, p_n$ using a block cipher `E` operating in `electronic code book (ECB) mode`, each ciphertext block $c_1, c_2, \ldots, c_n$ is computed as $c_i = E_k(p_i)$.

    Which of the following **is not** a property of this block cipher mode?

    (a) Any repeated plaintext blocks will result in identical corresponding ciphertext blocks.

    (b) Decryption can be fully parallelized.

    (c) If a ciphertext block is modified or corrupted, then after decryption the corresponding plaintext block and all the following plaintext blocks will be affected.

    (d) None of the above; that is, (a), (b), and (c) are all properties of the `ECB block cipher mode`.

11. (**2 pts.**) To encrypt a series of plaintext blocks $p_1, p_2, \ldots, p_n$ using a block cipher `E` operating in `cipher block chaining (CBC) mode`, each ciphertext block $c_1, c_2, \ldots, c_n$ is computed as $c_i = E_k(p_i \oplus c_{i-1})$, where c_0 is a public initialization vector (`IV`) which should be different for each encryption session.

    Which of the following **is** a property of this block cipher mode?

    (a) Any repeated plaintext blocks will result in identical corresponding ciphertext blocks.

    (b) Decryption can be fully parallelized.

    (c) If a ciphertext block is modified or corrupted, then after decryption the corresponding plaintext block and all the following plaintext blocks will be affected.

    (d) None of the above; that is, neither (a), (b), nor (c) are properties of the `CBC block cipher mode`.

12. (**2 pts.**) `Message authentication codes (MAC)` and `digital signatures` both serve to authenticate the content of a message. Which of the following best describes how they differ?

    (a) A `MAC` can be verified based only on the message, but a `digital signature` can only be verified with the secret key used to sign the message.

    (b) A `MAC` can be verified based only on the message, but a `digital signature` can only be verified with the public key of the party that signed the message.

    (c) A `MAC` can only be verified with the secret key used to generate it, but a `digital signature` can be verified based only on the message.

    (d) A `MAC` can only be verified with the secret key used to generate it, but a `digital signature` can be verified with the public key of the party that signed the message.

13. (**2 pts.**) Communication between end systems is encrypted using a

    (a) master key
    (b) permanent key
    (c) session key
    (d) message key

14. (**2 pts.**) Given plaintext NOWISTHEWINTEROF, which of the ciphertexts below result from a columnar transposition (circle all that apply)?

    - NSWEOTIRWHNOIETF
    - NWSHWNEOOITEITRF
    - NWOIWNITSETRHOEF
    - MNVHRSGDVHMSDQNE

15. (**2 pts.**) `Meet-in-the-middle` attack against `double DES` is

    (a) Cipher-text only crypto analysis
    (b) Known plaintext crypto analysis
    (c) Chosen cipher text crypto analysis
    (d) Chosen plaintext crypto analysis
    (e) None of the above

16. (**2 pts.**) In an unprotected network environment any client can apply to any server for service. The obvious security risk of this is

    (a) impersonation
    (b) certification
    (c) authorization
    (d) authentication

17. (**2 pts.**) The cryptographic hash function requirement that guarantees that it is impossible to find an alternative message with the same hash value as a given message and prevents forgery when an encrypted hash code is used is

    (a) second preimage resistant
    (b) collision resistant
    (c) pseudorandomness
    (d) preimage resistant

18. (**2 pts.**) A common item of authentication information associated with a user is a

    (a) nonce
    (b) timestamp
    (c) password
    (d) ticket

Question 1.3 (16 Points)

Given are two protocols in which the sender's party performs the following operation:

Protocol A:

$$y = E_{k_1}\Big(E_{k_{pub,r}}(x)||H(k_2||x)\Big),$$

where x is the message, H is a hash function, E is a symmetric-key encryption algorithm, "||" denotes simple concatenation, k_1, k_2 are secret keys which are only known to the sender and the receiver, and $k_{pub,r}$ is a public key of the receiver.

Protocol B:

$$y = E_k\Big(E_{k_{pub,r}}(x)||sig_{k_{pr,s}}\big(H(x)\big)\Big),$$

where k is a shared secret key only known to the sender and the receiver, $k_{pr,s}$ is a private key of the sender (not shared with the receiver), and $k_{pub,r}$ is a public key of the receiver.

(a) For each protocol, provide a step-by-step description (e.g., with an itemized list) of what the receiver does upon reception of y. [$k_{pub,s}$ is a public key of the sender, $k_{pub,r}$ is a public key of the receiver]

(b) State whether the following security services is given for each of the two prescribed protocols.

- confidentiality
- integrity
- non-repudiation (preventing an entity from denying previous commitments or actions)

Scratch Page - This page is intentionally left blank

Question 1.4 (8 Points)

Given the following fragment of code that implements the login functionality for a database application. The code dynamically builds an SQL query and submits it to a database.

```
String login, password, pin, query
login = getParameter("login");
password = getParameter("pass");
pin = getParameter("pin");
Connection conn.createConnection("MyDataBase");
query  = "SELECT accounts FROM users WHERE login='"+
         login + "'AND pass ='"+ password +
         "'AND pin = "+pin;

ResultSet result = conn.executeQuery(query);
if (result!=NULL)
  displayAccounts(result);
else
  displayAutFailed();
```

1. Suppose a user submits `login, password`, and `pin` as `doe, secret`, and `123`. Show the SQL query that is generated.

2. Instead, the user submits for the login field the following:

   ```
   ' or 1 = 1 --
   ```

   What is the effect?

Question 1.5 (20 Points)

A company is implementing `Bell-Lapadula model` for access control. Below are the access control matrix and the classifications of various objects and people. After going through them answer the following questions. Make sure to show the decision process that lead to your answer.

	`Salaries`	`Vacations`	`Building map`	`Orientation`
`Bob`	write, read	-	read	read
`Chris`	-	write, read	read	read
`Amy`	write, read	-	read	write, read
`Laura`	read	-	write, read	-

- There are three levels: *secret* > *confidential* > *normal*.
- `Amy` and `Chris` are cleared as *confidential*
- `Bob` is cleared as *secret*
- `Laura` is cleared as *normal*
- Files `Salaries` and `Vacations` are classified *secret*
- File `Building map` is classified *confidential*
- File `Orientation` is classified *normal*

(a) Which files can `Chris` read?

(b) Who can read the file `Building map`?

(c) Who can write on file `Vacations`?

(d) How can we grant to `Laura` permission to read the `Vacations` and `Orientation` files?