NATIONAL UNIVERSITY OF SINGAPORE

CS2107 ---- INTRODUCTION TO INFORMATION SECURITY

(Semester 2: AY2023/24) **Semester 1: AY2024/25**

December 2024

Time Allowed: 2 hours

INSTRUCTIONS TO CANDIDATES

- This is a **CLOSED BOOK** assessment. You are allowed to bring in 3 sheets of A4 paper written on both sides. You are allowed to use calculators.
- This assessment paper contains 38 questions and comprises 12 printed pages.
- Answer **ALL** questions. Each question worth 1 mark.
- Shade your answers and student ID on the **OCR ANSWER SHEET** using 2B pencil. Do not write your name.
- Hand in the OCR answer sheet. Do not hand in this question paper.

Remarks.

- In this paper, we assume that:
  - It is feasible to carry out 2^{64} primitive cryptographic operations.
  - It is infeasible to carry out 2^{100} primitive cryptographic operations.
  - It is feasible to carry out 2^{25} online dictionary attack.
  - It is infeasible to carry out 2^{30} online dictionary attack.
- Choose the most suitable answer. Quoted statements are modifications of phrases extracted from the public domain or other documents. They may not use the same notations in our lecture.

(Terminologies)

1. *"A basic rule of cryptography is to use published, public, algorithms and protocols; there should be no secrecy in the algorithm. This is generally known as ________."*

   a. security by design
   b. security by obscurity
   c. principle of the least privilege
   d. forward secrecy
   [✓ e.] Kerckoffs's principle

2. "___________ *is a centralized function within an organization employing people, processes, and technology to continuously monitor and improve an organization's security posture while preventing, detecting, analyzing, and responding to cybersecurity incidents*".

   a. Chief Information Security Officer (CISO)
   b. Security Information and Event Management (SIEM)
   [✓ c.] Security Operating Center (SOC)
   d. Intrusion Detection System (IDS)
   e. Virtual Private Network (VPN)

3. "______ *provides a reference-method for publicly known InfoSec vulnerabilities and exposures."*

   a. Black listing
   b. White listing
   c. NIST's guideline
   d. ISO
   [✓ e.] CVE

4. *“Our exploit acquisition program pays premium bounties and rewards to security researchers to acquire their original and previously unreported research affecting major operating systems, software, and/or devices. We pay the highest rewards on the market for* ________.”

   a. ransomwares
   b. botnets
   c. DDOS-as-a-service
   [✓ d.] zero-day vulnerabilities
   e. OS vulnerabilities

5. To choose a more secure system, the defender should choose one that can prevent attackers who ______

   [✓ a.] want to achieve an ***easier*** goal and have ***more*** capabilities.
   b. want to achieve a ***more difficult*** goal and have ***lesser*** capabilities.
   c. want to achieve an ***easier*** goal and have ***lesse***r capabilities.
   d. want to achieve a ***more difficult*** goal and have ***more*** capabilities.
   e. are very determine and smart.

(Credential and key strength)

6. Alice originally chose her password based on random combinations of a few words from a dictionary. A brute-force dictionary attack (which was aware of Alice’s dictionary) took 3 days to find the password. The time required to test a password is the same for any password. Suppose Alice enhanced her original method by doubling its “strength”. Specifically, she first employed the original method to independently choose two passwords p_1 and p_2. Next, the concatenated string ($p_1 \| p_2$) was chosen as the enhanced password. The attacker knew Alice’s enhanced method. How long would the new brute-force dictionary attack take to find the enhanced password?

   a. 6 days.
   b. 9 days.
   c. Unable to predict because there was missing information on the size of the dictionary. We can predict if such information is available.
   [✓ d.] Unable to predict because there was missing information on the time required to test one password. We can predict if such information is available.
   e. Both c and d are correct.

7. Suppose an organization decided to have 256-bit symmetric key for encryption. To achieve equivalent security, what should be the size of the hash digest?

a. 128 b. 256
c. 257 d. 384
[✓ e.] 512

8. Let us consider the security of hash function against quantum computer. We know that birthday attack can find collisions in $2^{n/2}$ operations where n is the digest length. Let us accept a claim by a research group that quantum computer can outperform birthday attack and find collisions in $2^{n/3}$ operations. Suppose an agency originally set a requirement of 256 bits for hash digest (without considering quantum computer). Now, in view of the threat from quantum computer, what should be the new requirement on the digest's length?

a. 128 b. 256
[✓ c.] 384 d. 512
e. 768

(Cryptography: DH, RSA, and general)

9. A Penguin appears in our lecture note. Which concept does it illustrate?
[✓ a.] Information leakage in ECB mode.
b. Malleability of CTR mode.
c. Padding oracle attack.
d. Predictability of IV.
e. Randomness of IV.

Q10 and Q11 are together.

10. Let us demonstrate Diffie Hellman (DH) key exchange with small integers. Choose g=2 and the modulo p= 11. Suppose Alice chooses her random secret a=2, and Bob chooses his random secret b=6, what is the final shared key?
a. 2 b. 3
[✓ c.] 4 d. 256
e. 4096

11. During key exchange, Alice sends a value to Bob. What is that value?
a. 0 b. 1
c. 42 [✓ d.] 4
e. 22

12. Under the attack model of DH key exchange, what is the attacker's capability with respect to sniffing, modification, injection and dropping of the messages?

[✓ a.] can sniff; can't modify; can't inject; can't drop.
b. can sniff; can modify; can inject; can drop.
c. can sniff; can't modify; can inject; can't drop.
d. can't sniff; can't modify; can inject; can't drop.
e. can't sniff; can't modify; can't inject; can drop.

13. With respect to C-I-A, what does DH key exchange aim to protect?

[✓ a.] "C"
b. "I"
c. "A"
d. Both "C" and "I".
e. All, i.e. "C", "I" and "A".

Q14 to Q18 are together

14. Consider classroom RSA where the modulo module n=55. What is the value of φ(n)? (recap that φ(n) =(p-1)(q-1))

a. 11, 5
b. 10, 4
c. 55
[✓ d.] 40
e. 15

15. Suppose n=55 and the encryption key e=7, what is the decryption key?

a. 1
b. 3
c. 8
d. 18
[✓ e.] 23

16. Suppose n=55, the encryption key e=7 and the plaintext m=1. What is the ciphertext?

a. 0
[✓ b.] 1
c. 7
d. 54
e. 56

17. Q16 illustrates one important issue on RSA that the lecturer stressed. What is this issue?

a. Decryption can be done much more efficiently than encryption.
[✓ b.] Classroom RSA has properties that could leak information and thus cannot be used as it is. Some forms of paddings are required.
c. Security of RSA relies on the computational difficulty in finding the plaintext, not the computational difficulty in finding the private key.
d. While working on small integers is easy, it is not clear how to compute exponentiation for very large, say 2000-bit integer.
e. RSA might not be secure and thus the industry in moving toward using ECC (Elliptic Curve Cryptography) based method.

18. Which statement below on the handling of φ(n) is correct?

    a. φ(n) *must be made public* since the public needs it for calculation.
    b. Although not necessary, φ(n) *can be made public*.
    [✓ c.] φ(n) *must not be made public*, otherwise the private key can be derived from the public key.
    d. So far, there is no known method that uses knowledge of φ(n) to break RSA. However, there is no formal proof to assure that such method does not exist. So, NIST recommendation is *not to make* it public.

19. Public key cryptography requires a secure broadcast channel to distribute the public keys. Consider the scenario where **A** intends to encrypt a plaintext which is to be decrypted by **B**. Which of the followings most accurately describes the consequences if the broadcast channel is being compromised?

    a. The attacker, from the ciphertext which is encrypted using **B**'s public key, could derive the plaintext. However, the attacker is unable to get **B**'s private key.
    b. The attacker, after received **B**'s public key, could derive the corresponding private key.
    c. The attacker could trick **B** to use a private key of the attacker's choice.
    [✓ d.] The attacker could trick **A** to use another public key (instead of **B**'s public key) to encrypt the plaintext.

(Cryptography: Hash, mac, signature)

20. We need a cryptographic secure hash function H() to be used in the hash-and-sign signature scheme. Among the 4 functions below, which one should we choose?

    a. A hash function that is one-way.
    [✓ b.] A hash function that is collision resistant.
    c. A hash function that is 2^{nd}-preimage resistant, i.e. given *x*, it is computationally difficult to find a *y* s.t. H(*x*)=H(*y*).
    d. A hash function that is balanced, that is, if *x* is a uniformly chosen 256-bit random string, then the *i*-th bit of H(*x*) has equal chances to be 0 or 1, for any *i*.
    e. A hash function that achieves forward secrecy.

21. Which of the following statement below is the most appropriate?

    a. Security of ***mac*** relies on the assumption that it is computationally infeasible to find collision.
    b. Security of ***signature*** relies on the assumption that it is computationally infeasible to find collision.
    [✓ c.] Security of ***hash*** relies on the assumption that it is computationally infeasible to find collision.
    d. Security of ***hash*** relies on the assumption that the attackers do not know a ***secret key***.
    e. Attack model of ***hash*** assumes that the attacker has many pairs of messages and their corresponding digests, and the attacker's goal is to ***forge*** a new message and its valid digest.

22. Which of the followings is the well-accepted way to protect password file?

    a. To protect ***confidentiality***, each password is ***encrypted*** with a randomly chosen IV (also known as the salt).
    [✓ b] To protect ***confidentiality***, each password is ***hashed*** with a randomly chosen salt.
    c. To protect ***integrity***, each password is ***signed*** with salt using mac.
    d. To protect ***integrity***, each password is ***signed*** with salt using signature.
    e. To protect both ***confidentiality and integrity***, each password is encrypted using ***authenticated-encryption*** (e.g. GCM mode).

23. Consider this hash function:

$$\mathrm{H}(m) = \mathrm{SHA3}\ (m) \oplus \mathrm{SHA3}\ (m \oplus \mathbf{1})$$

where **1** is a string of one's and it has the same length as *m*. Essentially, the operation ($m \oplus \mathbf{1}$) flips all the bits in *m*. To illustrate, `1011` ⊕ `1111` = `0100`. Which of the following statements is correct?

    a. Since SHA3 is collision resistant, so the following hash,
    $$\mathrm{H}'(m) = \mathrm{SHA3}\ (m \oplus \mathbf{1}),$$
    is also collision resistant. Since the xor'ed of two collision resistant functions is still collision resistant, and thus H() is collision resistant.

    b. Since H() is the xor of two functions, running time of birthday attack can be further reduced by another square root factor.

    [✓ c.] H() is not collision resistant. Simply choose any message *m*. Note that its digest is the same as the digest of ($m \oplus \mathbf{1}$).

    d. There exists a *m* and *m'* such that H(*m*) = H(*m'*) and m≠m'. Hence it is not collision resistant.

(Network Security)

24. The marketing material of a company claimed that:

    "WPA2-personal provides E2E and thus can prevent MITM while a user is surfing Internet".

    You were asked to comment on the above claim. Which of the followings is a correct and most precise comment?

    a. WPA2-personal employs an authenticated key-exchange that is vulnerable to offline dictionary attack. So, it is unable to provide E2E.
    [✓ b.] WPA2-personal does not provide E2E between the surfer's browser and the web server. This is because messages are already decrypted before reaching the web server. Thus, it is still possible to have MITM.
    c. WPA2-personal does not use public key cryptography, so it is unable to provide E2E.
    d. WPA2-personal protects communication between laptop to the WiFi router in the link layer. Only the laptop and WiFi router have the key. Hence, it indeed provides E2E and prevent MITM while surfing Internet.
    e. While the design of WPA2-personal provides E2E, there are many pitfalls in implementation.

<u>Q25, Q26 & Q27 are together</u>.

25. Alice used her laptop to access Internet via a free open WiFi (i.e. without protection such as WPA2) in a café. She conducted online banking with the website `https://bank.com`. Alice concurrently played an online game (over https) while visiting the bank website. Bob was in the café sitting in a nearby corner. Bob could:

    a. derive the fact that Alice visited the bank website.
    b. successfully conduct ARP attack and the above.
    [✓ c.] derive how many packets were sent by Alice to the bank and all the above.
    d. obtain Alice's bank account's password and all the above.
    e. none of the above.

26. The setting was the same as Q25. However, in this question, the café's WiFi was protected by WPA2-personal. Bob didn't know the WiFi's password. We assume that the password was sufficiently long to prevent offline dictionary attack. Bob could:

    a. derive the fact that Alice visited the bank website.
    b. successfully conduct ARP attack and the above.
    c. derive how many packets were sent by Alice to the bank and all the above.
    d. obtain Alice's bank account's password and all the above.
    [✓ e.] none of the above.

27. The setting was the same as Q25. However, in this question, the café's WiFi was protected by WPA2-enterprise. Both Alice and Bob had valid (and different) accounts. Recap that a separate authenticated key-exchange would be carried out for each session based on the café's public/private key. Let us assume that Alice laptop had a mechanism capable in detecting ARP attacks. Bob could:

    a. derive the fact that Alice visited the bank website.
    b. successfully conduct DNS spoofing and the above
    c. derive how many packets were sent by Alice to the bank and all the above.
    d. obtain Alice's bank account's password and all the above.
    [✓ e.] none of the above.

28. Suppose **M** was a MITM between **A** and a web server **S**. **M** successfully conducted re-negotiation attack. Suppose **A** originally (without the attack) intended to send a message "`XXX:000:A`" to **S**. Among the choices, which was the possible message received by **S** after the attack.

    a. `att>XXX:000:A:att`
    [✓ b.] `att>XXX:000:A`
    c. `    XXX:000`
    d. `att>XXX:000`
    e. Any of the above was possible.

29. Consider the DNS spoofing attack in our lectures. Recap that to spoof a valid reply, the attacker needs to know the QID in the query, which is only 16 bits long. Suppose the length of QID is changed to 100 bits, would the attack still work?

    a. The attack cannot be carried out now. It is infeasible to search over the message space.

    b. The attack can still be carried out. The attacker can exhaustively enumerate all possible 100-bit QID.

    [✓ c.] The attack can still be carried out. The length of the QID will not affect the attack effectiveness. This is because the attacker can see the QID value in the query and cut-and-paste into the query.

    d. The attack can still be carried out. The attacker can employ birthday attack that reduce the search space by a square root factor to 2^{50}.

    e. The attack cannot be carried out now. Online attack is only feasible if the search space is less than 2^{30}. Even if birthday attack is employed, that is still larger than 2^{30}.

(Secure Programming & Web)

30. Buffer overflow is an attack on the memory's _______.

    a. confidentiality
    [✓ b.] integrity
    c. availability
    d. forward secrecy
    e. perfect secrecy

31. Stack smack is a special type of _____ on the call stack.

    a. side channel attack
    b. unsafe function vulnerabilities
    c. row hammer attack
    [✓ d.] buffer overflow attack
    e. integer overflow attack

32. A webpage `cs2107.exam.com` included an "user feedback" section for any visitor to enter comments. The entered comments would be visible to other visitors. Instead of entering sensible feedbacks, a malicious visitor entered comments in the form "`<script>`*code*`<script>`" where *code* was some javascripts. It turned out the script could be executed in other visitors' browsers. This was an example of:

    a. Reflection XSS.
    [✓ b.] Persistent XSS.
    c. Cross-site request forgery (Sea-surf).
    d. SQL injection.
    e. All the above.

Q33 and Q34 are together.

33. Consider the following C program:

```
int main() {

unsigned char total;   // 8-bit unsigned integer.
unsigned char str[1024];

scanf ("%1000s", str); //read in a string of at most 1000 characters

total = strlen(str);   //return number of characters in str
total = total + 10;

if (total <  10)  printf ("AAA”);
if (total >= 10)  printf ("BBB");
}
```

We had learned in tutorial that, for `str` of certain length, the program will print out “AAA”. Among the following lengths, which will cause “AAA” to be printed out.

a. 5 b. 127
c. 128 [✓ d.] 250
e. none of the above.

34. This is a repeat of Q33. Among the following lengths, which will cause “AAA” to be printed out.

[✓ a.] 510 b. 520
c. 530 d. 540
e. none of the above.

(Access Control)

35. In an online forum, by default all users can read any post created by any user. Nonetheless, the creator of each post can specify a list of users who cannot read that post. This is an example of ________.

a. principle of least privilege
b. role base access control
c. mandatory access control
[✓ d.] discretionary access control
e. Intermediatory control

Q36, Q37 and Q38 are together.

36. Two systems, **A** and **B**, classify the users into two classes: *trusted* or *untrusted*, and the files as *sensitive* or *non-sensitive*. System **A** adopts **Biba** whereas **B** adopts **Bell-LaPadula** to control read/append to the files. In which system a trusted user is permitted to append to a sensitive file?

    [✓ a.] In **A** and **B**.
    b. In **A** only.
    c. In **B** only.
    d. None.

37. Consider the same setting in Q36. In which system an untrusted user is permitted to read a non-sensitive file?

    [✓ a.] In **A** and **B**.
    b. In **A** only.
    c. In **B** only.
    d. None.

38. Consider the same setting in Q36. Suppose each file is a list of instructions to be executed by the users who read the file. To protect the trusted users from running compromised instructions, which system should be deployed?

    a. Irrelevant. The access control model is about protection of information, not about protection of processes.
    b. Either **A** or **B** is suitable.
    [✓ c.] **A** only.
    d. **B** only.

--------------------- END-OF-PAPER -----------------------