NATIONAL UNIVERSITY OF SINGAPORE

CS2107 ---- INTRODUCTION TO INFORMATION SECURITY

(Semester 2: AY2023/24)

May 2024

Time Allowed: 2 hours

INSTRUCTIONS TO CANDIDATES

- This is an **OPEN BOOK** assessment. You are allowed to bring in material of your choice into the assessment hall, including hardcopies, calculator, laptop, and tablet. You can use them when answering the questions.

- All types of network connection must be turned off, except Bluetooth that connects input devices such as mouse. You are **NOT** allowed to use mobile phone. Cameras and audio recording are **NOT** allowed. You are **NOT** allowed to use preloaded LLM.

- This assessment paper contains 32 questions and comprises 14 printed pages.

- Answer **ALL** questions. Each question worth 1 mark.

- Shade your answers and student ID on the **OCR ANSWER SHEET** using 2B pencil.

- Hand in the OCR answer sheet. Do not hand in this question paper.

Remarks: In this paper, we assume that:
(1) It is feasible to carry out 2^{64} primitive cryptographic operations.
(2) It is infeasible to carry out 2^{128} primitive cryptographic operations.
(3) It is feasible to carry out 2^{25} online dictionary attack.
(4) It is infeasible to carry out 2^{30} online dictionary attack.

(General)

1. During your job interview in a security company specializing in monitoring health-informatic network, after knowing that you completed security modules in NUS, the interviewer was excited and mentioned "*S O C level 2* ". The interviewer most likely was referring to:

   a. The area outsides COM1 SR1 in School of Computing.
   b. Higher level security protocols in System-On-Chip.
   [✓ c.] Higher lever tasks in a Security Operating Center.
   d. System and Organization Control for cybersecurity level 2 compliance.

2. _____________ is a list of entries -- each containing an identification number, a description, and at least one public reference – for publicly known cybersecurity vulnerabilities.

   a. NIST
   [✓ b.] CVE
   c. MITRE
   d. Zero-day vulnerabilities
   e. Cyber Threat Intelligent (CTI) report.

3. In ______, the vulnerability was not caused by programming bug or design flaw. It was a backdoor intentionally planted by a malicious programmer.

   a. Mirai attack
   [✓ b.] XZ Utils
   c. zero-day
   d. Padding Oracle attack
   e. Integer overflow attack

4. An attacker registered a domain name "Gooogle.com", and next set up a spoofed "Google.com" website. The attacker was hoping that some Internet users would incorrectly type "Gooogle.com" into their web browser. This is an example of ______.

   a. Phishing attack
   [✓ b.] Typosquatting attack.
   c. Side-channel attack.
   d. Skimmer attack.
   e. TLS attack.

(Password, key strength)

5. 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.

6. An agency recommended 70 bits entropy to guard against password ***offline*** dictionary attack. Now, in view of the threat of quantum computer, what should be the revised recommendation?

   a. 70 bits
   b. 71 bits
   c. 72 bits
   [✓ d.] 140 bits
   e. 4900 bits

7. An agency recommended 30 bits entropy to guard against password ***online*** dictionary attack. Now, in view of the threat of quantum computer, what should be the revised recommendation?

   [✓ a.] 30 bits
   b. 31 bits
   c. 32 bits
   d. 60 bits
   e. 900 bits

8. Alice chose her password based on random combinations of words from a dictionary. A brute-force dictionary attack (which was aware of Alice's dictionary) took 5 days to find the password. Suppose Alice enhanced her choice of password 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 brute-force dictionary attack take to find the enhanced password?

   a. 10 days.
   b. 7 days
   c. 5^2 days.
   d. 2^5 days.
   [✓ e.] Unable to predict because there was missing information.

(Cryptography)

9. Alice needed to choose a symmetric key encryption for her applications. She gathered a few candidates, each claimed to meet certain security requirements. Among the followings, which one should Alice choose?

   a. Claimed to be secure against known plaintext attack.
   b. Claimed to be secure against ciphertext only attack.
   c. Claimed to be secure against birthday attack.
   d. Claimed to be secure against encryption oracle.
   [✓ e.] Claimed to be secure against decryption oracle.

10. Which of the following statements on collision is correct?

   [✓ a.] Any hash function, whether cryptographically secure or not, has many collisions.
   b. A MAC that is collision resistant is a cryptographically secure MAC.
   c. If a hash function is one-way, then it must be collision resistant.
   d. A collision of SHA3 has been found.
   e. A secure encryption scheme must be collision resistant.

11. Consider a hash function H(***x***) = SHA3(***x***) ⊕ SHA3(*compl*(***x***)), where *compl*() is the complement operation that flips every bit. For example, *compl* (‘00110’) gives ‘11001’. Which of the followings most accurately describes security of H()?

   a. No new information on SHA3(***x***) is being leaked by SHA3(*compl*(***x***)). Therefore H() inherits all security properties of SHA3. Since SHA3 is collision resistant and one-way, then so is H().
   b. Suppose an attacker can find a collision of H(), the collision can be easily transformed to a collision of SHA3, contradicting SHA3 is secure. Therefore, H() is collision resistant.
   c. It may happen that SHA3(***x***) is the same as SHA3(*compl*(***x***)), which lead to a digest of all zeros. Hence, it is not collision resistant.
   [✓ d.] For any ***x***, H(***x***) = H(*compl*(***x***)) even when ***x*** is not the same as *compl*(***x***). It is easy to construct such a ***x***. Hence, we can easily find many collisions and thus H() is not collision resistant.
   e. By pigeonhole principle, there exists many pairs of ***x*** and ***y*** such that H(***x***) = H(***y***). So, H() is not collision resistant.

Q12, Q13, Q14 are together.

12. A question was posted in the public forum Stack Overflow:

> "*What is the difference between hashing a password (using SHA3 with salt) and encrypting it (using AES-CBC mode with random IV)? Which way is recommended for password file protection?*"

You want to post an answer. You want to support using ***hash***. Which of the followings is a sensible and most precise reason.

[✓ a.] Encryption has the disadvantage that the key must be securely stored. If the attacker happens to obtain both the password file and the key, all passwords will be revealed.
b. Encryption does not have salt, and hence vulnerable under rainbow table attack.
c. Encryption is vulnerable to Grover's search and thus not quantum safe.
d. There are many side-channel attacks on encryption.
e. In term of security, both are equivalent since it is computationally infeasible to invert. Nonetheless, encryption/decryption is much slower than hash. Hence for efficiency consideration, use hash.

13. This is a continuation of the previous question. Instead of hash, you want to support using ***encryption***. Which of the followings is a sensible and most precise reason?

a. Hash has the disadvantage that collision is inevitable. There is no guarantee that there is no collision among the passwords.
b. It is not possible to recover the original password using hash. On the other hand, with encryption, it is possible.
[✓ c.] For weak passwords, it is still feasible for an attacker to recover the passwords from their digests, even if salted. However, without knowing the key, it is infeasible to recover the weak passwords from the ciphertext.
d. Hash is vulnerable to birthday attack, which essentially reduce the security strength by half.
e. In term of security, both are equivalent since it is computationally infeasible to invert. Nonetheless, hash is much slower than encryption/decryption. Hence for efficiency consideration, use encryption.

14. This is a continuation of the previous question. Instead of supporting either hash or encryption, you want to recommend doing ***both***. Which of the followings is a sensible and most precise reason?

a. Following the principle of defense-in-depth, it is always not less secure to have additional layer of defense.

b. Following the principle of least privilege, it is advisable to employ a combination of multiple protections.

c. It is more secure to have the respective advantage in both previous 2 questions. For each password, one should store ($\boldsymbol{c}$, $\boldsymbol{s}||\boldsymbol{d}$) where $\boldsymbol{c}$=Enc(k,$\mathbf{p}$) is the cyphertext (together with the IV), $\boldsymbol{s}$ is the salt, $\boldsymbol{d}$ is the salted hash, and k is the encryption key.

[✓ d.] It is more secure to have the respective advantage in both previous 2 questions. For each password $\boldsymbol{p}$, one should store ($\boldsymbol{s}||\boldsymbol{c}$) where $\boldsymbol{c}$=Enc(k,H($\boldsymbol{s}||\boldsymbol{p}$)), where k is the encryption key. In other words, encrypt the salted hash.

<u>IOT: Q15 and Q16 are together.</u>

15. An IoT device can receive remote instructions. The length of each instruction is 128 bits. Not all possible 128-bit strings are valid instructions. A total of 2^{100} strings are valid instructions. After the device receives an instruction, it checks whether it is valid. If not, the device will drop the instruction. An attacker can send a total number of ***M*** instructions to the device. However, due to some technical constraint, the attacker can only send randomly chosen strings. Among the choices of ***M*** below, which is the smallest so that with high probability (more than 0.5), at least one of the strings is a valid instruction?

[✓ a.] 2^{30}

b. 2^{50}

c. 2^{64}

d. 2^{100}

e. 2^{128}

16. Refer to Q15. A new version of the IoT device employs AES encryption. Each instruction is encrypted using AES CBC mode with randomly chosen IV. When the device receives the instruction, it decrypts and check whether the plaintext is a valid instruction. If not, the device will drop the instruction. Similarly, the attacker can send ***M*** random strings (each string consists of the IV and the ciphertext) to the device. Among the choices of ***M*** below, which is the smallest so that with high probability (more than 0.5), at least one of the plaintexts is a valid instruction?

[✓ a.] 2^{30}

b. 2^{50}

c. 2^{64}

d. 2^{100}

e. 2^{128}

17. Alice clicked on a link and visited a website. The browser gave a warning that the certificate was expired. The browser also indicated that the CA's signature in the certificate was valid when verified using the CA's public key. Furthermore, the browser double checked that the certificate was not revoked. Alice made sure that there is a padlock and the url was correct. Alice decided to go ahead and visited the website. It turned out that the website was spoofed. Among the followings, which was ****not**** a likely scenario?

a. The browser contained a vulnerability and did not verify the certificate correctly. The operator of the spoofed website exploited that vulnerability.

b. The domain name changed owner. The spoofed website was operated by the previous owner.

c. The private key was stolen after the certificate expired. Hence, the rightful owner did not revoke the certificate. The spoofed website was operated by the attacker who stole the private key.

[✓ d.] It is easier to forge an expired certificate because the attacker would have a much longer time to find the private key from the public key. The website was operated by an attacker who had spent considerable computing resources to forge one such expired certificate.

e. Alice's laptop previously was tricked to accept a self-signed certificate of a malicious CA. This expired certificate was signed by this malicious CA and the same attacker operates the spoofed website.

(Network Security)

Questions Q18 to Q22 are together. Alice was in a café with wifi, and Bob sat a few tables away. Recap that under WPA2 personal, there is only one common password for all users.

18. The wifi was protected by WPA2 personal. Alice knew the password. Bob didn't know the password. The password consisted of 8 alphanumeric characters. Alice submitted her report to Canvas. Would Bob able to get the report?

[✓ a] No. Canvas is protected by TLS which is above the link layer. WPA2 is for the link layer. So, even if WPA2 was compromised, protection by TLS would still be in place.

b. No. Entropy of 8 alphanumeric characters is more than 30, which is sufficient to guard against online dictionary attack.

c. Yes. Entropy of 8 alphanumeric characters is less 60, and so Bob can successfully carry out offline dictionary attack.

d. Yes. Bob could become a MITM between Alice and Canvas, and then get the report.

e. Yes. Bob could conduct padding oracle attack to get the report.

19. The wifi was protected by WPA2 personal. Alice knew the password. Bob didn't know the password. The password consisted of 8 alphanumeric characters. Alice wanted to connect to Canvas. Would Bob able to carry out DNS spoofing attack?

a. No. Since WPA2 provides protection in the link layer and Bob at best could be a MITM in the physical layer. So, Bob was unable to carry DNS spoofing in the application layer.

b. No. Bob was unable to obtain the QID in the DNS query, and thus unable to spoof a valid DNS reply.

c. Yes. Bob can carry out online dictionary attack to obtain Alice's WPA2 session key. With that, Bob became MITM and thus could carry out DNS spoofing attack.

[✓ d.] Yes, and it would take a few steps. Bob first carried out offline dictionary attack to get the Wifi password. Next, Bob carried out ARP attack to become MITM. After that, Bob could carry out DNS spoofing.

e. Yes. No cryptographic scheme is perfect. With sufficient compute resources and time, one could break the protocol and then carry out DNS spoofing.

20. The wifi was protected by WPA2 personal. Alice knew the password. Bob also knew the password. The password consisted of 20 alphanumeric characters. Under WPA2, different WPA2 session keys would be established for different wifi sessions. Alice successfully connected to the wifi. Would Bob be able to find out Alice session key?

    a. No. Authenticated key exchange is designed to guard against MITM in link or lower layer. Whether Bob knew the password, or the strength of the password would not matter since WPA2 is in the link layer.
    b. No. 20 alphanumeric is sufficient to guard against both online and offline dictionary and thus Bob is unable to get the session key.
    c. Yes. With sufficient time, Bob can carry out dictionary attack to obtain Alice's WPA2 session key.
    d. Yes. All communication would be encrypted using the password. Since Bob also knew the password, Bob could obtain the session key.
    [✓ e.] That depended on whether WPA2 authenticated key-exchange achieved forward secrecy. If not, since Bob knew the password, Bob could intercept the key-exchange and then derive the WPA2 session key. If yes, then Bob was unable to get the session key.

21. The wifi was protected by WPA2 personal. Alice and Bob knew the password. Could Bob successfully carry out ARP attack?

    a. No. WPA2 Authenticated key exchange was designed to guard against MITM in link or lower layer. Whether Bob knew the password, or the strength of the password would not matter since WPA2 was in the link layer.
    b. No. Since different sessions would be established, Bob was unable to observe the ARP resolution process and thus unable to carry out ARP attack.
    c. No. That depends on the password strength. If it was sufficiently strong, Bob would not be able to derive the session key. As a result, Bob was unable to observe the ARP resolution process and thus unable to carry out ARP attack.
    [✓ d.] Yes. ARP attack consisted of a few steps on top of the link layer. Whether the wifi was protected by WPA2 or not was irrelevant with respect to ARP attack. Since both Alice and Bob would be in the same network, Bob could carry out ARP attack.
    e. Yes. From the authenticated key-exchange, Bob could derive the Alice's WPA2 session key. Now, with the session key, Bob could inject ARP instructions accepted by the WPA2's protocols.

22. The wifi was not protected. Alice connected to Canvas through NUS VPN. Would Bob find out that Alice was visiting Canvas?

    a. No. VPN established a digital connection between Alice and a server in NUS, creating a point-to-point tunnel that encrypts Alice's personal data.

    b. No. NUS VPN was above the link layer, hence, the ip header would be encrypted before passing to the link layer. It would be decrypted at the VPN server in NUS. Bob would only get frames encrypted by VPN.

    c. Yes. NUS VPN was on top of the IP layer. So, Bob can see the ip address in the header, and thus knew that Alice is connected to Canvas.

    d. Yes. The wifi was not protected and thus Bob could see all the frames and ip packets. From there, Bob could extract the ip address of Canvas. In fact, the ip addresses must be in clear, otherwise, it is impossible to connect to Canvas.

    [✓ e.] It depends on how the DNS query was served. If DNS request was not routed to NUS, Bob could intercept the unprotected DNS and derive that Alice was visiting Canvas. If not, Bob would only get frames encrypted by VPN and no knowing that Canvas was being visited.

23. When a user, say Alice, visits Canvas, Alice needs to enter her password. We know that TLS/SSL's handshake is being carried out. Which of the following is a correct and most precise description of the overall authentication process?

    a. It is a unilateral authentication that verifies the website's authenticity.

    b. It is a unilateral authentication that verifies Alice's authenticity.

    c. It is a TLS mutual authentication. Both Alice and the website use each other public key to verify authenticity of each other.

    d. It is a TLS mutual authentication. Alice uses the website public key to verify the website authenticity, and the website uses Alice's password to verify Alice's authenticity.

    [✓ e] It is a mutual authentication. A TLS unilateral authentication is first carried out to verify the website site. Next, in the application layer, Canvas uses password to unilaterally verify Alice authenticity.

24. Certain conditions are required to carry out re-negotiation attack. Which of the followings correctly describe the condition?

    a. The attacker is an eavesdropper in the network layer. That is, the attacker can inspect the IP packets but cannot modify them.
    b. The attacker is a MITM in the network layer with some limited capability. The attacker can inspect the IP packet, inject IP packets, but not dropping nor modify them.
    [✓ c.] The attacker is a MITM in the network layer. The attacker can inspect the IP packet, inject IP packet, and modify them.
    d. The attacker is a MITM in the application layer. The attacker can inspect and modify the url, html, and cookies exchanged between the client and server.
    e. The attacker is an eavesdropper in the application layer. That is, the attacker can inspect the url, html, and cookies exchanged but cannot modify them.

25. Which of the followings is most precise and accurate description of the re-negotiation attack?

    a. It is due to programming error and should be considered as an issue in secure programming.
    b. It is due to a flaw in the design of some cryptographic primitives.
    [✓ c.] It is due to a flaw in the protocol design.
    d. It is due to some overlooked security assumptions as in side-channel attack. The attacker exploits some additional information that was not considered in the original design.
    e. It is due to an access control configuration mistake.

(Secure Programming)

26. Consider this statement,

```
strncpy (B, A, 10);
```

in a C program. Here, `strncpy` copies null-terminated string from `A` to `B` and the number of bytes copied is bounded by at most 10 bytes. Suppose 10 bytes is allocated/reserved for the array `B`, `A` is a null-terminated string with 10 characters "`0123456789`", and `B` is to be treated as null-terminated string in other parts of the program. Would this potentially lead to vulnerability?

[✓ a.] Yes. By the specification of `strncpy`, in the above, 10 bytes will be copied to `B`. However, the null character will not be copied to `B`. Hence, after the copying, `B` might not be null terminated.

b. Yes. String has variable length. There is no guarantee that in another part of the program, `B` is used to store a shorter string.

c. No. The number of bytes is bounded, and hence `B` will not be overflown/overran.

d. No. `strncpy` is a safe function.

e. It depends on the original content in `B`. If `B` originally contains only null character, then `strncpy` might cause segmentation fault.

27. Consider the IP address example on "Data Representation" in Topic 6 (Secure Programming). Suppose the ip address 100.3.1.2 is blacklisted, among the following possible inputs, which would bypass the check and yet 100.3.1.2. would be connected?

a. `100.3.1.2`

b. `2.1.3.100`

[✓ c.] `100.2.257.2`

d. `100.31.2.0`

e. `100.3.0.256`

28. Alice wrote a C program. She complied it using gcc with the default parameters on her Linux machine. The complied executable was then run in a version of Linux. Alice noticed that the stack canaries was on. Her original intention was to demonstrate stack smack in a presentation. Thus, the canary had to be off. What changes should she make?

a. Modify the C program to disable canary.

[✓ b.] No change to the C program. Recompile the program but with some suitable gcc parameters.

c. No change to the C program. Modify the OS configuration, and then recompile the program (with the default gcc parameter).

d. No recompilation required. Run the executable in the original version of Linux but with some suitable changes to the OS configuration.

e. Using debugger to remove the canary from the executable.

(Access Control)

Q29,Q30 and Q31 are together.

29. A Massively Multiplayer Online (MMO) game platform classifies the gamers in a team into two types: *core* or *normal* players. Core players trusted each other. Each team keeps a pool of documents, and each document is classified as *sensitive* or *non-sensitive*. Sensitive documents contain important information on game strategies and resource status. During the design of this MMO, Biba and Bell-LaPadula were considered.

    Under which design a *core* player is permitted to append to a *sensitive* file?

    [✓ a.] Both Biba and Bell-LaPadula.
    b. Biba only.
    c. Bell-LaPadula only.
    d. None.

30. Consider the same setting in the previous question. Under which design a *normal* user is permitted to read a *non-sensitive* document?

    [✓ a.] Both Biba and Bell-LaPadula.
    b. Biba only.
    c. Bell-LaPadula only.
    d. None.

31. Consider the same setting in the previous question. Under which design a *normal* user is permitted to append to a *sensitive* document?

    a. Both Biba and Bell-LaPadula.
    b. Biba only.
    [✓ c.] Bell-LaPadula only.
    d. None.

32. In an online forum, all users can read any post created by any user. The creator of the post cannot exclude any specific user from reading the 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

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