# 香 港 中 文 大 學
# The Chinese University of Hong Kong

## 二零二一至二二年度上學期科目考試
## Course Examination 1st Term, 2021-22

科目編號及名稱
Course Code & Title : IERG4130 Introduction to Cyber Security

時間 小時 分鐘
Time allowed : 2 hours 0 minutes

學號 座號
Student I.D. No. : ..... Seat No. : .....

**SPECIAL NOTES:**

1. For oversea students who are *approved* to attend the online exam conducted at the same exam time, you must follow "ExamInstructions." Failure to do that will affect your scores.
2. This exam carries 100 raw marks in total, and consists of 11 questions in THREE pages.
3. Please write down your answers in the ANSWER SHEET. Please manage your time well.

**PART I: Web/Software Security. [5 questions, 8 marks each. Answers of Q1-Q3 are short.]**

1. To launch effective CSRF attacks, what are the two user-related conditions that are required at the victim user side?

2. Can the same-site cookie countermeasure for CSRF attacks defeat XSS attacks? Why?

3. Assume that a database only stores the sha256 value for the pwd and eid columns. The following SQL statement is sent to the database, where the values of the $pwd and $eid variables are provided by users. Does this program have a SQL injection problem? Why?

```
SELECT * FROM employee WHERE eid='SHA2($eid, 256)' and pwd='SHA2($pwd, 256)';
```

4. In the buffer overflow example in Lecture 11 Page 38 (also listed in next page), is this statement true or false? "*The buffer overflow occurs inside the strcpy() function, so the jumping to the malicious code occurs when strcpy() returns, not when foo() returns.*" Please explain.

```
/* stack.c */
/* This program has a buffer overflow vulnerability. */
#include <stdlib.h>
#include <stdio.h>
#include <string.h>

int foo(char *str)
{
    char buffer[100];

    /* The following statement has a buffer overflow problem */
    strcpy(buffer, str);

    return 1;
}
```

5. Please draw the function stack frame for the following C function. (Hint: your drawing should start from the function parameter *str* and end at the 24-byte *buffer* array.)

```
int bof(char *str)
{
    char buffer[24];
    strcpy(buffer,str);
    return 1;
}
```

**PART II: Cryptography and Network Security. [6 questions, 10 marks each. Q6 is short.]**

6. What are the two fields (with random value) in a DNS query packet that need to be included in the DNS response/reply packet?

7. Let G:$\{0, 1\}^l \rightarrow \{0, 1\}^n$ be a secure PRG (Pseudorandom Generator). Is $F(k) = G(k)||G(k)$ a secure PRG? If it's a secure PRG, please give a brief explanation; if it's not, please provide an attack and compute its adventange. [The "||" here means connecting two bit sequences.]

8. In the RSA algorithm, since doing $(M^e)^d$ mod n and $(M^d)^e$ mod n always get the same result $M$. Bob decides to keep $e$ as the private key and use $e$ to do the decryption, and publish $d$ as the public key, and use $d$ to do the encryption. Is this safe? Why?

9. Given $h = Sha256(K \,||\, M)$, where $K$ is a secret and "||" means concatenation (no padding is involved in calculating $h$). Can you calculate $Sha256(K \,||\, X)$ for a different message $X$ without knowing $K$? If yes, what condition does $X$ need to satisfy?

10. Owing to the fact that block encryption and cryptographic hash functions generate discrete output sizes, an IPSec packet can take only some legitimate sizes. In this question, IPSec uses the ESP in the transport mode, and uses the 16-byte **block** size for encryption (e.g., using AES) and the 64-byte hash's **output** size for message authentication (e.g., SHA-512). The IP header is also 20 bytes long (i.e., without IP option). Is the following IPSec packet size legitimate or not? "The IPSec packet size (including the IP header) is 212 bytes". And why? (hint: the 16-byte IV and the 64-byte hash should be considered in this question.)

11. Given the following X.509 certificate, please answer three subquestions (2 + 4 + 4 marks).

```
Certificate:
 Data:
  Version: 3 (0x2)
  Serial Number:
    2a:a1:f0:37:0b:84:e0:78:dc:16:12:a6:a0:1e:22:ed
 Signature Algorithm: sha256WithRSAEncryption
  Issuer: C=GB, ST=Greater Manchester, L=Salford, O=Sectigo Limited,
          CN=Sectigo RSA Domain Validation Secure Server CA
  Validity
    Not Before: Feb 26 00:00:00 2020 GMT
    Not After : Apr 25 23:59:59 2022 GMT
  Subject: CN=www.cuhk.edu.hk
  Subject Public Key Info:
    Public Key Algorithm: rsaEncryption
      Public-Key: (2048 bit)
      Modulus:
      00:b7:5b:da:7d:1a:5b:5f:32:32:cc:7c:2f:bc:6c:
      b3:5e:3c:ac:0f:a8:d0:32:ef:63:f6:19:5d:bd:26:
      ...
      Exponent: 65537 (0x10001)
 Signature Algorithm: sha256WithRSAEncryption
    0d:14:2f:65:3a:25:ce:c9:48:39:2e:94:7b:e3:47:9e:8b:08:
    ea:f5:0a:05:98:c0:90:35:67:87:e7:c1:75:47:3d:1e:77:eb:
    ...
    c4:e6:3f:da:6e:0f:df:09:92:0c:75:e8:a0:3f:70:90:fe:de:
    ea:6b:e2:74
```

a) What should be used to verify this signature? (please give the precise name)

b) The public key contained in this certificate is based on RSA. Using the RSA algorithm, to encrypt a message $M$, we calculate $M^e mod\ n$. What is the value of $e$ and $n$ in this public key? If the number is too long, you only need to write down its first four bytes.

c) Before issuing the certificate, the CA needs to do a verification regarding the subject field. Please describe what this verification is, and why it is necessary.

- End of the Question paper -