NATIONAL UNIVERSITY OF SINGAPORE

CS2107 — INTRODUCTION TO INFORMATION SECURITY

(Semester 2: AY 2018/19)

Time Allowed: 2 Hours

INSTRUCTIONS TO STUDENTS

1. Write your Student Number only. Do not write your name.

2. This assessment paper contains **FOUR** questions and comprises **FOURTEEN** printed pages.

3. Answer **ALL** questions.

4. Write your answer within the given box in each question. You may use pencil. Give your answers on the provided answer sheet for Q1.

5. This is an Open Book assessment.

Student Number: ☐☐☐☐☐☐☐☐☐

Question	Full Marks	Marks	Remark
Q1	34		
Q2	22		
Q3	23		
Q4	21		
Total	100		

Notations and Assumptions.

- Attackers know the algorithms and systems (i.e. Kerckhoff's principle).

- $\text{Enc}_k(m)$, $\text{Hash}(m)$, $\text{MAC}_k(m)$ are symmetric key encryption, hash and mac respectively, where k is the secret key. We assume that these cryptographic functions are secure.

- $\langle x, y \rangle$ refers to a 2-tuple. The actual data representation format is of no interest here.

Q1. **[34 marks] Multiple Choice Question.** Give the *most* appropriate choice. 2 marks each. Shade your answers on the provided answer sheet using pencil.

1. A _____ hacker hacks under good intentions with permission.

   (A) black hat

   (B) white hat

   (C) grey hat

   (D) blue team

   (E) red team

2. A _____ 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) SIEM

   (B) SOC

   (C) CISO (chief information security officer)

   (D) Intrusion detection system

   (E) Firewall

3. Let us consider the Github attack presented in tutorials. The java injection attack would not be possible if,

   (A) the Github's servers employed effective filtering rules that detect cross-site-scripting attacks.

   (B) the Baidu's servers employed effective filtering rules that detect cross-site-scripting attacks.

   (C) the communication between Baidu and its users was secured using HTTPS.

   (D) the communication between the users and Github was secured using HTTPS.

   (E) the users were careful in clicking urls listed in their emails.

2

4. Heartbleed attack illustrated that a remote malicious client

   (A) could overwrite the server's memory by exploiting buffer overflow.

   (B) could read the server's memory by exploiting buffer "over-read".

   (C) could compromise memory confidentiality by exploiting stack smacking.

   (D) could compromise execution integrity by exploiting buffer overflow.

   (E) could compromise memory integrity by exploiting integer overflow.

5. An application adopted an outdated version of TLS that was vulnerable to re-negotiation attack. This application facilitated data transfer from a IoT device to a client. The transfer was be done in the following steps:

   i. The client and device established TLS connection using unilateral authentication (authenticating the device).

   ii. The client sent an instruction m.

   iii. The device sent data x to the client.

   Suppose a client sent the instruction $m =$ "hand?op1=100". By exploiting re-negotiation attack, a MITM could:

   (A) obtain the instruction m.

   (B) obtain the data x, even though the MITM did not know m.

   (C) replay m a few hours later, even though the MITM did not know m.

   (D) modify the instruction m so that the server would receive "hand?op1=101".

   (E) modify the instruction m so that the server would receive "upperhand?op1=100".

6. Bob had coded and built an application using C++. Bob did his work on a laptop whose os was not updated. Bob's supervisor noticed that the application was not protected by stack canaries, and tasked Bob to fix the problem. To achieve that, Bob should:

   (A) modify his C++ program by inserting canaries in each function.

   (B) recompile his C++ program using a compiler that supported stack canaries.

   (C) update the operating system and recompile his C++ program.

   (D) add a check in the application to make sure that the users had the correct version of operating systems.

   (E) remove all function calls in the C++ program.

The next 5 questions are based on the following files.

```
-r-s---r-x   1 alice    year1  May 2 2019 01:00 program1
-r-s---r-x   1 bob      year2  May 2 2019 01:00 program2
-r-s---r-x   1 root     staff  May 2 2019 01:00 program3
-r-x---r--   1 root     staff  May 2 2019 01:00 program4
-r--------   1 root     staff  May 2 2019 01:00 data.txt
```

7. If user alice executes program1, what will be the effective and real UID of the process?

    (A) Effective: root, Real: alice.

    (B) Effective: root, Real: root.

    (C) Effective: alice, Real:root.

    (D) Effective: alice, Real: alice.

    (E) alice does not has access right to execute the file.

8. If user alice executes program2, what will be the effective and real UID of the process?

    (A) Effective: bob, Real: alice.

    (B) Effective: bob, Real: bob.

    (C) Effective: alice, Real:alice.

    (D) Effective: root, Real: alice.

    (E) alice does not has access right to execute the file.

9. If the user alice execute that file program4, what will be the effective and real UID of the process?

    (A) Effective: bob, Real: alice.

    (B) Effective: bob, Real: bob.

    (C) Effective: alice, Real:alice.

    (D) Effective: root, Real: alice.

    (E) alice does not has access right to execute the file.

10. If user `bob` executes `program2`, does the process has read access to the file `data.txt`?

   (A) Yes.

   (B) No.

   (C) Yes, if the process does not modify its real and/or effective UIDs. Otherwise, could be "no" in certain scenarios.

   (D) No, if the process does not modify its real and/or effective UIDs. Otherwise, could be "yes" in certain scenarios.

   (E) `bob` does not has access right to execute `program2`.

11. If user `alice` executes `program3`, does the process has read access to the file `data.txt`?

   (A) Yes.

   (B) No.

   (C) Yes, if the process does not modify its real and/or effective UIDs. Otherwise, could be "no" in certain scenarios.

   (D) No, if the process does not modify its real and/or effective UIDs. Otherwise, could be "yes" in certain scenarios.

   (E) `alice` does not has access right to execute `program3`.

The next 3 questions are based on the following scenario. Alice was connected to Internet using Bob's wifi router. The wifi was protected using WPA2-personal. It was well-known that WPA2-personal was vulnerable to dictionary attack. Alice logged into IVLE (over https) to submit her report. Let us assume that Alice's laptop was free from vulnerabilities, and Bob was familiar with known hacking techniques.

12. Bob wanted to extract as much information about Alice as possible. Bob could obtain:

   (A) The fact that Alice was visiting `ivle.nus.edu.sg`.
   (B) The type of browser (e.g. Chrome or Firefox) Alice was using.
   (C) Alice's report.
   (D) Alice's userid.
   (E) None of the above.

13. Alice IVLE's password was only 10 digits long and Bob knew Alice's userid. Could Bob obtain the password? (Note that $\log_2 10^{10} \approx 33$).

   (A) Yes. Although the traffic was encrypted, Bob could sniff the encrypted packets and carry out offline dictionary attack.
   (B) Yes. Bob could exhaustively tried all possible passwords to log into IVLE. Since 10^{10} is not large, Bob would eventually get the correct password.
   (C) No. The password was encrypted using SSL's session key, and Bob was only able to get the encrypted password.
   (D) No. Alice's password was hashed with salt. It was computationally difficult for Bob to invert the salted hash.
   (E) No. The entropy of Alice's passwords was more than 30 bits, which was sufficient for passwords.

14. Eve was stationed near Bob's wifi access point and she didn't know the wifi password. The wifi password was also 10 digits long. Could Eve obtain the wifi password?

   (A) Yes. Eve could sniff a handshake between Alice and the access point, and then carry out offline exhaustive search over the 10-digit passwords.
   (B) Yes. Eve could exhaustively tried all possible passwords to log into the wifi access point. Since 10^{10} is not large, Eve would eventually get the correct password.
   (C) No. The wifi password was never sent in clear over air.
   (D) No. The wifi password was hashed with salt. It is computationally difficult to invert the salted hash.
   (E) No. The passwords' entropy (≈ 33) was sufficiently large.

15. There are many forms of authentication. When we visit `https://ivle.nus.edu.sg`, what type of authentication will be carried out by the TLS protocol?

   (A) Unilaterally-authenticated key exchange where the web server is being authenticated.

   (B) Unilateral authentication where the web server is being authenticated.

   (C) Unilateral-authenticated key exchange where the client is being authenticated.

   (D) Unilateral authentication where the client is being authenticated.

   (E) Mutually-authenticated key exchange.

16. The firewall of an organization blocks off connection between the SQL server and the Internet, and it only allows selected nodes such as the Web Server and a few administrators' workstations to be connected to the SQL server. This design illustrates the concept of:

   (A) Kerckhoff's principle.

   (B) security by obscurity.

   (C) principle of least privilege.

   (D) role-based access control.

   (E) access control list (ACL).

17. A webpage `cs2107.exam.com` contained an "user feedback" section for any visitor to enter comments. The entered comments would be visible to other visitors. Instead of entering constructive feedbacks, a visitor entered comments in the form "`<script>` *code* `<script>`" where *code* was some javascripts. It turned out the script *code* 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.

Q2. [**22 marks**] Short Questions.

(a) (8 marks) Consider the scenario for Q1.12 on Bob's wifi. Suppose Alice was using a sufficiently long password, but Alice's browser contained a bug: the browser would not verify the authenticity of a certificate if its expiry date was in year 1999. Bob was aware of this bug. Describe how Bob would able to steal the password.

(b) (7 marks) Javascript in browser can be very expressive. For instance, they can extract information from cookies, refresh a page, send information to another webserver, display graphic on the browser, etc. Consider question Q1.17. Explain how it is possible for an attacker to steal cookies stored by `cs2107.exam.com` even if the "same-origin policy" is enforced.

(c) (7 marks) Suppose $\langle S_{pub}, S_{pri} \rangle$ were the respective public and private key of Superfish. Explain why S_{pri} had to be stored in the Lenovo laptops.

A researcher discovered that S_{pri} was stored in a particular file. Instead of storing S_{pri} as plaintext in the file, the ciphertext $\text{Enc}_k(S_{pri})$ was stored, where k was a 128-bit key. It turned out that k was derived from a short string s and the researcher easily found s (which was the word "komodia") using dictionary attacks. Now, let us consider a hypothetical situation where k is a 128-bit string generated by some secure random generator. In such situation, would the smart researcher able to recover S_{pri}?

Q3. **[23 marks]** The university plans to install a booking system for tables in library. Each table would be equipped with a tampered-proofing IoT device that equips with a small display panel. Each IoT device has a 4-byte identity ip which is essentially its ip-address. All the IoT devices keep a shared 128-bit secret key k. A server S also has the same key k.

When the table is available, the panel will display a QRcode carrying the message $m_0 = \langle ip, t, \text{Hash}(\langle ip, t \rangle) \rangle$, where t is current date and time rounded to the nearest minute. If Alice wants to book the table, Alice carries out the following steps:
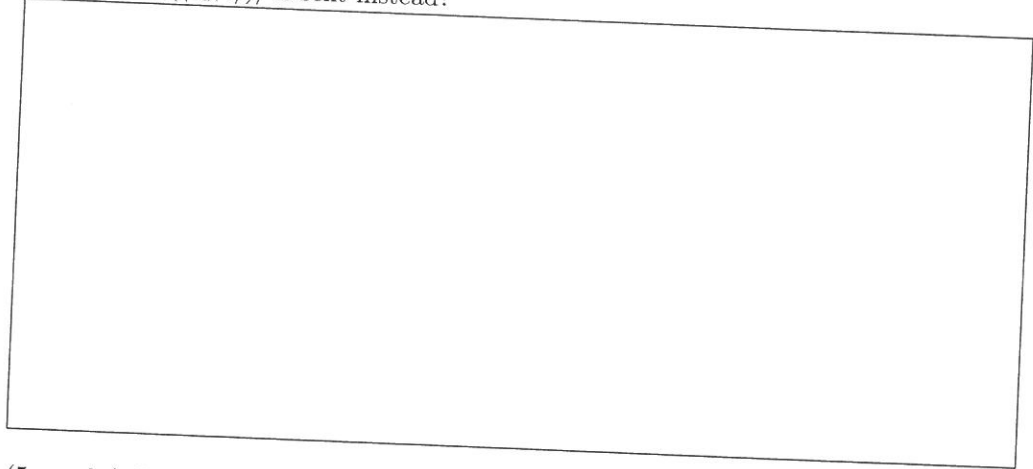
(P1) Alice scans the QRcode and obtains m_0.

(P2) Alice sends $\langle m_0, I_a \rangle$ to S, where I_a is Alice's student identity number.

(P3) S verifies that current time is closes to t and Alice has not booked another table. If so, it sends a UDP packet containing $\langle I_a, t, \text{MAC}_k(\langle I_a, t, ip \rangle) \rangle$ to the IoT device. It also update its database to take note that Alice has booked a table.

(P4) The IoT device verifies that the information it received from S is authentic, and the table is currently not booked. If so, it displays I_a.

We assume that the channel in step (P2) between Alice and S is secure (for e.g. Alice logged-in via HTTPS). Every booking will last for one hour.
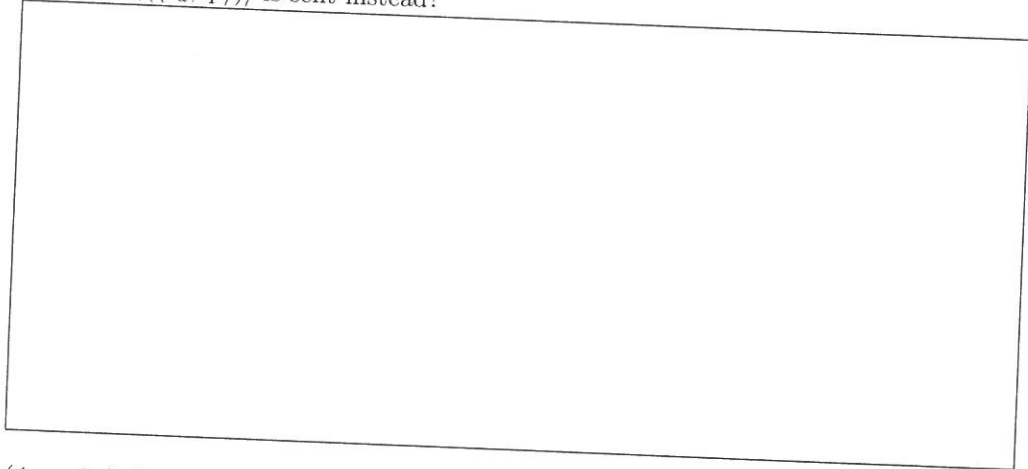
(a) (5 marks) The university wants to prevent students from booking the tables while not physically near the tables. Explain why this system cannot prevent that.

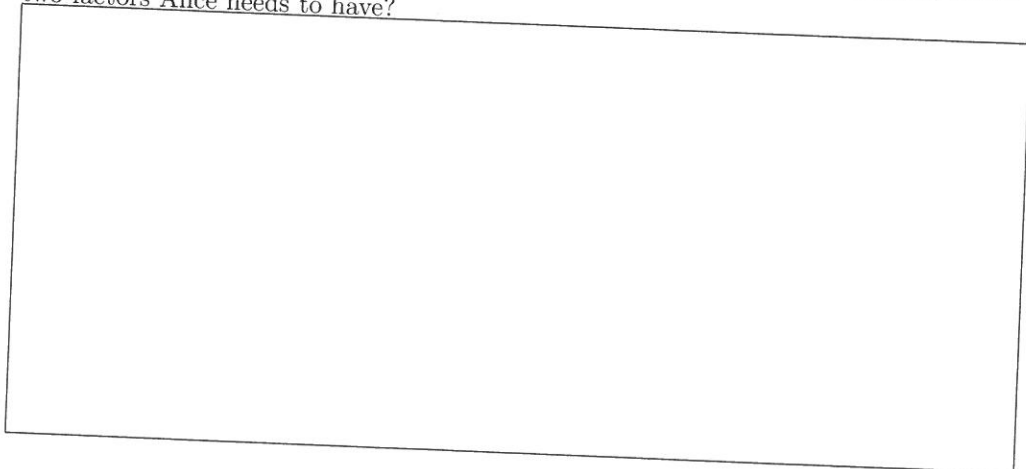(b) (4 marks) Give a way to fix the limitation described in Question Q3(a).

(c) (5 marks) What would be the consequence if step (P3) omits ip, i.e., the message $\langle I_a, t, \mathrm{MAC}_k(\langle I_a, t \rangle) \rangle$ is sent instead?

(d) (5 marks) What would be the consequence if step (P3) omits t, i.e., the message $\langle I_a, \mathrm{MAC}_k(\langle I_a, ip \rangle) \rangle$ is sent instead?

(e) (4 marks) One could argue that this protocol illustrates 2FA. To book a table, which two factors Alice needs to have?

11

Q4. [21 marks]

(a) (7 marks) Consider the following C program snippet.

```
unsigned char B[1500];
unsigned char A[50];
unsigned char C;                       // one-byte non-negative integer.
RU(B);                                 // (L1)
C = strlen (B);                        // (L2)
if (C <=  50)                          // (L3)
  { strncpy (A, B, C);                 // (L4)
     for (int i=0; i< strlen (B) ; i++)// (L5)
        {printf("%d\n", A[i]);}        // (L6)    displaying for user
  }
```

The library routine RU obtains a null-terminated string from the user, and stores it in B. RU carries out input validation properly and it makes sure that the string length of B is at most 1024, and it contains only numeric characters. If error occured, RU will store a null string in B, i.e. B[0] will be the null character. We assume that the routine RU is correctly implemented.
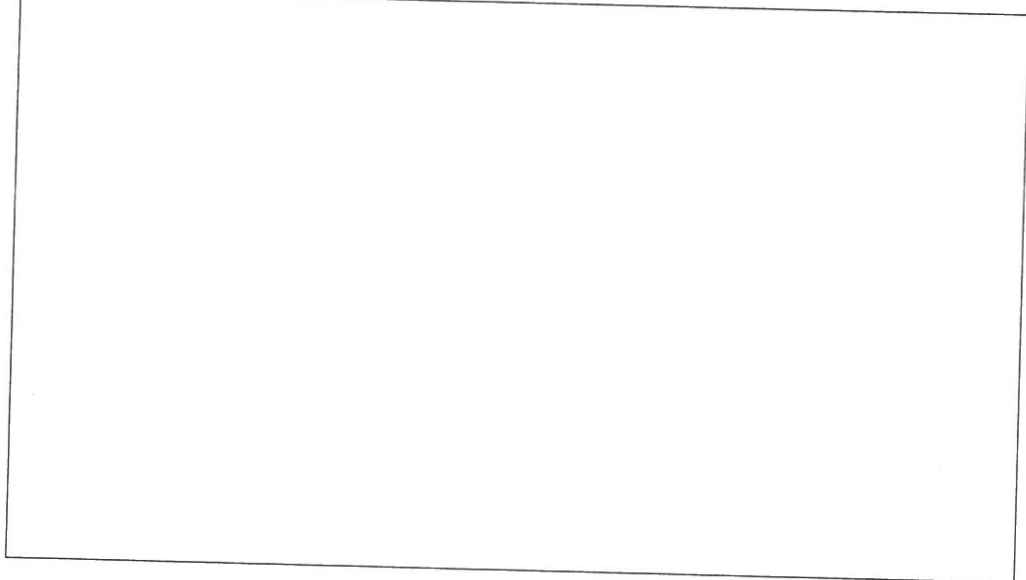
A malicious user can craft the input to trigger undesired outcomes. Describe how this is possible.

Describe all possible choices of the input that will trigger the malicious outcomes.
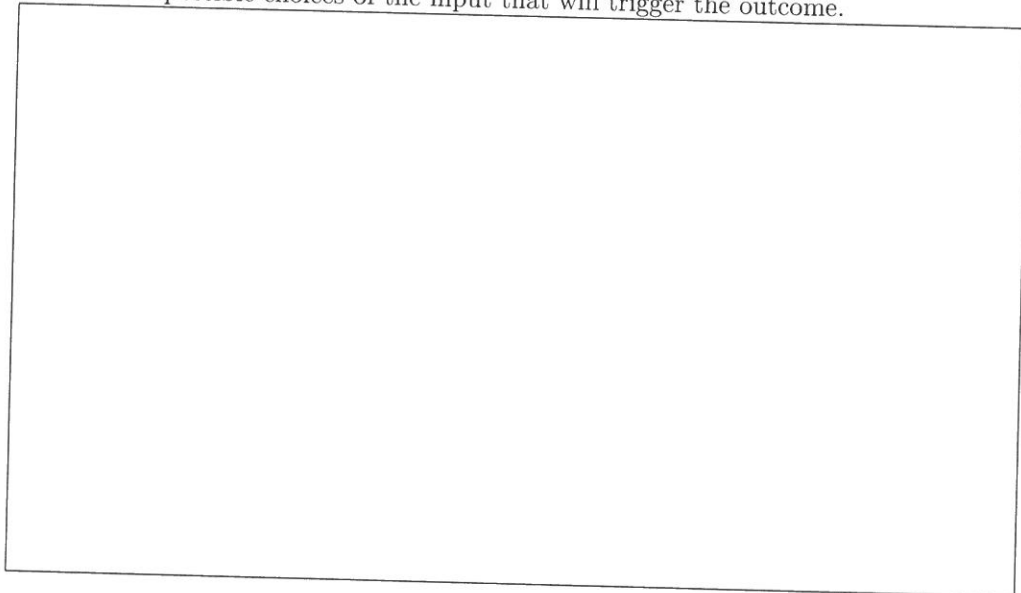
(b) (7 marks) In an updated version, line (L5) and (L6) are being replaced by

```
printf ("%s \n", A);                // (K5)
```

Explain why the updated version is still vulnerable.

Describe all possible choices of the input that will trigger the outcome.
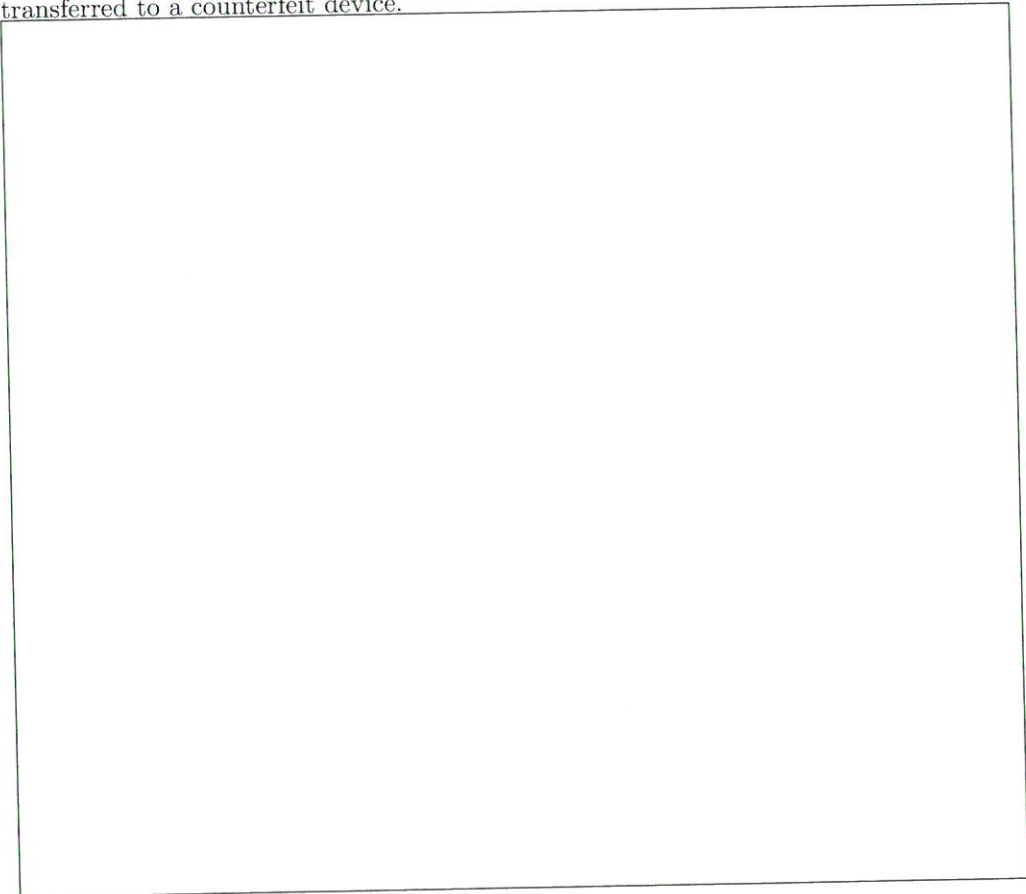
(c) (7 marks) Consider the following C program snippet.

```
{ unsigned char F[100000];
  if ( VerifyUSB (i) )    \\ (L1)    return 1 (true) if it is not counterfeit
    { Construct(F);       \\ (L2)    Prepare the data to be transferred
      SendUSB (i, F);}    \\ (L3)    Transfer the data
}
```

Let us suppose that a system file keeps information of the devices plugged into the USB ports. Whenever a device is plugged in or out, the information in the file will be updated immediately. The routine VerifyUSB(i) reads that system file, and verifies whether the device connected to the i-th USB port is a genuine product. We omit the details of the verification process. The routine SendUSB(i,F) opens the i-th USB port and write data to the port.

This code intends to prevent data being transferred to counterfeit devices. Unfortunately, the code is vulnerable. Explain and give the condition whereby data can be transferred to a counterfeit device.

— End-Of-Paper —