Queen Mary
University of London

Main Examination Period: 2018

ECS655U-ECS775P Security Engineering Duration: $2\frac{1}{2}$ hours

YOU ARE NOT PERMITTED TO READ THE CONTENTS OF THIS QUESTION PAPER UNTIL INSTRUCTED TO DO SO BY AN INVIGILATOR.

Instructions: This paper contains FOUR questions. **Answer ALL questions**. Cross out any answers that you do not wish to be marked.

Calculators are not permitted in this examination.

Complete all rough workings in the answer book and cross through any work that is not to be assessed.

Possession of unauthorised material at any time when under examination conditions is an assessment offence and can lead to expulsion from QMUL. Check now to ensure you do not have any notes, mobile phones, smartwatches or unauthorised electronic devices on your person. If you do, raise your hand and give them to an invigilator immediately.

It is also an offence to have any writing of any kind on your person, including on your body. If you are found to have hidden unauthorised material elsewhere, including toilets and cloakrooms it will be treated as being found in your possession. Unauthorised material found on your mobile phone or other electronic device will be considered the same as being in possession of paper notes. A mobile phone that causes a disruption in the exam is also an assessment offence.

Exam papers must not be removed from the exam room.

Examiners: Dr Arman Khouzani, Dr Na Yao

Question 1

(a) (i) Provide a short definition for each of the following security services:

- Confidentiality
- Data integrity

[4 marks]

(ii) For each of the above security services, determine whether a "digital signature" scheme alone provides that service.

[2 marks]

(b) Briefly, provide one similarity and one difference between symmetric-key and public-key cryptosystems. **[6 marks]**

(c) Recall that in the basic RSA public-key cipher, the encryption of the message m, and decryption of the ciphertext c can be expressed as follows:

$$\text{Encryption: } c = m^e \mod n$$
$$\text{Decryption: } m = c^f \mod n$$

(i) From above, identify which parameter/parameters constitute the private key, and which parameter/parameters constitute the public key.

[3 marks]

(ii) Express the two computationally infeasible problems that underpin the security of RSA, and describe the attack scenario each of them are related to.

[3 marks]

(d) Consider the following diagram describing the encryption algorithm in a particular mode of operation of a block cipher like AES, and answer the subsequent questions.

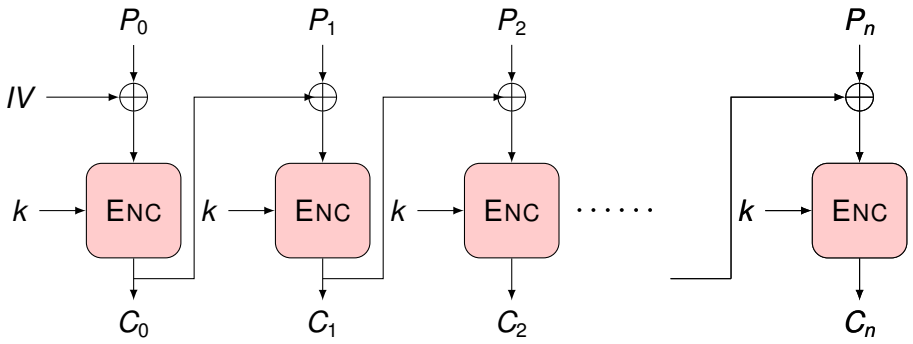

Figure 1: Q. 1-(c). Notations: $P_0,\ldots,P_n$: blocks of plaintext. IV: Initialization Vector. $C_0,\ldots,C_n$: blocks of ciphertext. k: cryptographic key. ENC: an encryption block. $\oplus$: XOR operator.

(i) Elaborate on the main *advantage* of using this mode of operation compared with the Electronic Code-Book (ECB) mode.

[4 marks]

(ii) Draw the diagram of the corresponding decryption process.

[3 marks]

Question 2

(a) Consider the following cryptographic protocol:

- Alice (the sender) and Bob (receiver) have established two symmetric keys k_1 and k_2. That is, k_1 and k_2 are "only" known by (both) Alice and Bob.
- Both parties have also already agreed on the choice of a strong symmetric-key encryption algorithm e, and a strong message-authentication-code algorithm MAC (e.g., a strong HMAC).
- Alice (the sender) performs the following on her message m, and sends the output y over to Bob over a public channel:

$$y = e_{k_1}\left(m || MAC_{k_2}(m)\right)$$

In case you need a reminder, the notations are as follows:

- $e_k(x)$ represents the symmetric-key encryption of a message x with key k using algorithm e;
- $MAC_k(x)$ represents the MAC of the message x computed using key k; and
- and $x||y$ represents simple concatenation (appending) of the two messages x and y together.

(i) Describe the corresponding process in the receiver; i.e., what does Bob do to y upon receiving it? **[3 marks]**

(ii) For each of the following security services, determine whether our protocol provides it. Each of your answers should be supported by a brief but clear justification:

- Confidentiality
- Data origin authentication
- Entity authentication
- Non-repudiation

[12 marks]

(b) Answer the following questions regarding digital signatures, specifically, the "RSA digital signature scheme with appendix":

(i) Provide two reasons why hashing is used as part of this scheme (why the message is first hashed before signing).

[3 marks]

(ii) Suppose Alice has the RSA key pair of $(K^A_{\text{private}}, K^A_{\text{public}})$ and Bob has the RSA key pair of $(K^B_{\text{private}}, K^B_{\text{public}})$. Alice wants to provide a digital signature on her message and send it to Bob. Specify which one of these 4 keys is used fore "signing" and which of these keys is used for "verification".

[3 marks]

(c) What is the role of the TLS handshake protocol? (What specific tasks does TLS handshake perform so that a secure TLS channel can be set up?)

[4 marks]

Question 3

(a) Briefly describe the difference between Mandatory Access Control (MAC) and Discretionary Access Control (DAC).

[5 marks]

(b) Describe the two rules of the “Bell-LaPadula” model in access control.

[4 marks]

(c) Consider the following c-code and answer the questions accordingly:

```
#include <stdio.h>
#include <string.h>

int main(void){
  char s[15];
  int success = 0;
  printf("Enter password : \n");
  gets(s);
  if(strcmp(s, "ECS655U775P")){
    printf ("Incorrect password! \n");}
  else{ success = 1;}
  if(success){
    /* Grant root privilege to the user*/
    printf ("Root privilege granted! \n");}
  return 0;
}
```

(i) Identify and describe the outstanding vulnerability in this program? (Hint: what happens if a long string of characters is passed at runtime?)

[4 marks]

(ii) How should the code be changed to remedy that vulnerability (Hint: the main culprit is the use of one function, identify which one)?

[4 marks]

(iii) How can the compiler and OS provide safety against such vulnerabilities?

[4 marks]

(d) Describe the principle of “least privilege” and how it helps improve security.

[4 marks]

Question 4

(a) Consider the following sample packet filtering rule-set of a firewall that we are using to protect our subnet. Recall that SMTP (Simple Mail Transfer Protocol) daemon runs on a server port of 25, and a client port of $>$ 1023, i.e., some port number strictly higher than 1023. This rule-set is hence designed to only allow emails in and out of our subnet.

Rule	Direction	Src. Addr.	Dest. Addr.	Protocol	Src. Port	Dest. Port	ACK	Action
A	In	External	Internal	TCP	$>$ 1023	25	Any	Permit
B	Out	Internal	External	TCP	25	$>$ 1023	Yes	Permit
C	Out	Internal	External	TCP	$>$ 1023	25	Any	Permit
D	In	External	Internal	TCP	25	$>$ 1023	Yes	Permit
E	Either	Any	Any	Any	Any	Any	Any	Deny

Table 1: An example packet filtering rule-set related to problem Q4.part(a). Note: Src.: Source, Dest.: Destination, Addr.: (IP) Address.

(i) Explain why we have set the ACK column of rule B as "Yes" (that is, what may happen if we had instead set the ACK of Rule B as Any)?

[4 marks]

(ii) Suppose we want to change the packet filtering rule-set so that it only allows emails to enter our subnet (and no longer emails are sent out from our subnet). Explain which rows we should remove (specified by its Rule letter in the first column of the table, from A...E). Provide your reasoning.

[6 marks]

(b) What does port scanning mean (what does it involve) and how it may help an attacker.

[5 marks]

(c) Describe any of the notions of input escaping, input validation and input sanitization (describing only one of them suffices). Then explain how specifically it can help against Cross-Site Scripting (XSS).

[6 marks]

(d) Explain the notion of usability-security trade off through an example.

[4 marks]

End of questions