Queen Mary
University of London

Late Summer Resit **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) Define each of the following security services, and for each of them mention one example cryptographic primitive that provides that security service on its own:

- Data Origin Authentication
- Non-repudiation

[5 marks]

(b) Provide one advantage and one disadvantage of a symmetric-key cryptosystems compared with a public-key cryptosystem.

[5 marks]

(c) (i) In order to establish "entity authentication" in a communication setting, briefly explain why we in part need a mechanism that ensures "freshness".

[5 marks]

(d) Answer the following questions about cryptographic hash functions.

(i) What is a cryptographic hash function? Describe the three security properties of a cryptographic hash function.

[5 marks]

(ii) Explain the danger of using a cryptographic hash function with a short output length (e.g. if the hash values are 64 bits long).

[5 marks]

Question 2

(a) Consider the following protocol between Alice (sender) and Bob (receiver):

- Both parties have already agreed on the choice of a strong cryptographic hash function H (e.g. SHA-512), and the choice of a strong public key cipher E, e.g. RSA-4096.
- Alice has a private-public key pair of (k^A_{priv}, k^A_{pub}) and Bob has the private-public key pair of (k^B_{priv}, k^B_{pub}).
- Only Alice knows k^A_{priv} and only Bob knows k^B_{priv}.
- Both k^A_{pub} and k^B_{pub} are publicly known.
- Alice (the sender) performs the following on her message m, and sends the output y to Bob over a public channel:

$$y = E_{k^B_{pub}}(m||H(m))$$

The notations are as follows:

- $E_{k^B_{pub}}(x)$ represents the public-key encryption of a message x with public-key of k^B_{pub} using algorithm E;
- $H(x)$ represents the cryptographic Hash of the message x using hash function H;
- and $x_1||x_2$ represents simple concatenation (appending) of the two messages x_1 and x_2 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 services, determine whether our protocol provides it. Each of your answers should be supported by a brief but clear justification:

- Confidentiality
- Data Integrity
- Detection of accidental changes (e.g. due to channel noise)
- Non-repudiation

[12 marks]

(b) Answer the following questions regarding public key certificates:

(i) What is the main purpose of a public key certificate (why is it needed?)

[3 marks]

(ii) What is a public key certificate composed of? Name at least 4 essential pieces of information does in a public key certificate.

[4 marks]

(c) Explain how using PIN verification when using an electronic payment card (e.g. visa/mastercard, etc) is an example of multi-factor authentication.

[3 marks]

Question 3

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

[5 marks]

(ii) Describe the two rules of the “Biba” model in access control.

[5 marks]

(iii) Identify which one of these two models is concerned with “confidentiality” and which one is concerned with “integrity”?

[3 marks]

(b) (i) In access control, describe an “Access Control List” (ACL) and a “Capability list” (C-List) with an example for each.

[4 marks]

(ii) Provide an advantage and a disadvantage of using Access Control Lists compared with Capability Lists.

[4 marks]

(c) What is the purpose of “address space layout randomization (ASLR)” in computer security?

[4 marks]

Question 4

(a) (i) Describe a Cross-Site-Request Forgery (CSRF) attack through an example scenario.

[5 marks]

(ii) Explain how CSRF tokens can help against CRSF attack.

[5 marks]

(b) Consider the following PHP code, that is the content of a page `/index.php`:

```
$myvar = "varname";
$x = $_GET['arg'];
eval("\$myvar = \$x;");
```

(i) Identify the most outstanding vulnerability and provide an example attack.

[5 marks]

(ii) What security measures can mitigate such vulnerabilities as in the above code? (name at least two).

[5 marks]

(c) Provide at least two security controls that can counter "social engineering" attacks like "phishing".

[5 marks]

End of questions