No calculator allowed in this examination

UNIVERSITY OF BIRMINGHAM

School of Computer Science

Introduction to Computer Security

Main Summer Examinations 2019

Time allowed: 1:30

[Answer all questions]

Note

Answer ALL questions. Each question will be marked out of 20. The paper will be marked out of 60, which will be rescaled to a mark out of 100.

Question 1

(a) What is a Block cipher mode? **[5 marks]**

(b) Assume a webserver is accessible only via TLS with Forward Secrecy. The operator of the webserver wants to enable a webfilter which checks all incoming traffic to the webserver for malware before it reaches the webserver.

(i) Why is this not possible if the webfilter only gets the private key of the webserver and a feed of the incoming traffic? **[4 marks]**

(ii) Which changes are necessary to make these checks possible? Justify your answer. **[4 marks]**

(c) Assume a webserver uses AES in counter mode. Furthermore assume the attacker has managed to install malware on the webserver which sets the nonce used in the counter mode to a value specified by the attacker. If the malware can in addition cause the webserver to encrypt data of the attacker's choice, can the attacker decrypt all traffic to the website? Justify your answer. **[7 marks]**

Question 2

(a) What is a replay attack? **[5 marks]**

(b) Is it safe to replace nonces by timestamps in a security protocol? Justify your answer. **[5 marks]**

(c) Consider the following protocol:

$$\begin{array}{lcl} A & \rightarrow & B : N_A, B \\ B & \rightarrow & A : E_A(N_A), E_A(Sign_B(\text{Pay Elvis } \pounds 5), \text{Pay Elvis } \pounds 5) \end{array}$$

Assume different protocol runs produce different payment messages. Is this protocol secure? If yes, explain why. If not, give an attack in Alice-Bob notation. **[5 marks]**

(d) Consider the following protocol:

$$\begin{array}{lcl} A & \rightarrow & B : E_B(N_A, A) \\ B & \rightarrow & A : E_A(N_B, B) \\ A & \rightarrow & B : E_B(N_B) \end{array}$$

where N_A and N_B are nonces, and $\#(N_A, N_B)$ is a symmetric key based on the hash of N_A and N_B. By giving an attack in Alice-Bob notation, show that this protocol does not satisfy key agreement. **[5 marks]**

Question 3

(a) What is a cookie? **[3 marks]**

(b) Browsers allow access to cookies only if the domain of the cookie is the same as the domain for the website. Describe an attack which is prevented by this restriction. **[4 marks]**

(c) A website uses https for authentication but the link to the general conditions of use on the same domain uses only http. How could an attacker get access to this website without authentication? **[4 marks]**

(d) Consider the following php-code running on a web server:

```
 1  <?php
 2  $filename = $_REQUEST["filename"];
 3  $command = "ls -l /var/www/img/" . "$filename";
 4
 5  system("$command". $result);
 6  if ($res <> 0) {
 7      echo File "$filename" already uploaded;
 8  }
 9  else {
10      mysqli_multi_query($con,"INSERT INTO pictures (username, filename)
11                VALUES (" . get_current_user() ", " . "$filename)");
12  }
13  ?>
```

Describe three security weaknesses in this website, how they might be exploited and explain why these weaknesses are serious. **[9 marks]**

End of Paper

This page intentionally left blank.

Do not complete the attendance slip, fill in the front of the answer book or turn over the question paper until you are told to do so

Important Reminders

- Coats/outwear should be placed in the designated area.
- Unauthorised materials (e.g. notes or Tippex) must be placed in the designated area.
- Check that you do not have any unauthorised materials with you (e.g. in your pockets, pencil case).
- Mobile phones and smart watches **must** be switched off and placed in the designated area or under your desk. They must not be left on your person or in your pockets.
- You are not permitted to use a mobile phone as a clock. If you have difficulty seeing a clock, please alert an Invigilator.
- You are not permitted to have writing on your hand, arm or other body part.
- Check that you do not have writing on your hand, arm or other body part – if you do, you must inform an Invigilator immediately
- Alert an Invigilator immediately if you find any unauthorised item upon you during the examination.

Any students found with non-permitted items upon their person during the examination, or who fail to comply with Examination rules may be subject to Student Conduct procedures.