UNIVERSITY OF BIRMINGHAM

School of Computer Science

Second - Year - BSc Artificial Intelligence and Computer Science
First Year - UG Affiliate Computer Science/Software Engineering
Second Year - BSc Computer Science
Second Year - MSci Computer Science
Second Year BEng/MEng Comp Science/Software Engineering
Second Year - MEng Computer Science/Software Engineering
Second Year - BSc Computer Science w Study Abroad
Second Year - MSci Computer Science w Study Abroad
BSc Computer Science w Business Management
Second Year - BSc Computer Science w Industrial Year
Second Year - MEng Comp Science/Software Engineering w Industrial Year
BSc Computer Science w Business Management w Industrial Year
Second Year - MSci Computer Science w Industrial Year
Second Year - BA/BSc Liberal Arts + Sciences

06 26265

Introduction to Computer Security

Main May/June Examinations 2018

Time allowed: 01:30

Answer ALL Questions.

Note
Each question will be marked out of 24. Up to 20 marks will be awarded for content, with up to 4 additional marks for the quality, coherence, and clarity of your answer. The examination will be marked out of 72, which will be rescaled to a mark out of 100.

1. (a) How does padding work? **[5 marks]**

   (b) For full disk encryption would you use AES in CBC-mode or in counter mode? Justify your answer. **[5 marks]**

   (c) Alice and Bob use the Diffie-Hellman key exchange protocol to derive a session key. If this is done over an unencrypted wireless connection, can an active attacker learn the session key? Either describe an attack, or explain why no attack exists. **[5 marks]**

   (d) Assume the account number is contained in the first block of a message. Assume CBC-mode is used for encryption. Is it possible for an active attacker to change the account number? Either describe an attack, or explain why no attack exists. **[5 marks]**

2. (a) What is a Man-in-the-middle-attack? **[5 marks]**

   (b) A website uses TLS to ensure credit card data is transmitted securely. Is this enough to protect against malware running on the client? Justify your answer. **[5 marks]**

   (c) Consider the following protocol:

$$\begin{array}{lcl} A & \rightarrow & B : A \\ B & \rightarrow & A : N_A \\ A & \rightarrow & B : \{N_A\}_{K_{ab}}, \{\text{Pay Elvis £5}\}_{K_{ab}} \end{array}$$

   where N_A is a nonce and K_{ab} is a symmetric key known only to Alice and Bob. Is this protocol secure? If yes, explain why. If not, give an attack in Alice-Bob notation. **[5 marks]**

   (d) Consider the following protocol:

$$\begin{array}{lcl} A & \rightarrow & B : N_A, A \\ B & \rightarrow & A : \{N_A, N_B, B\}_{pk(A)} \\ A & \rightarrow & B : \{M\}_{\#(N_A, N_B)} \end{array}$$

   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, and $pk(A)$ is the public key of A. Is it possible for the attacker to learn M without knowing the private key of A? If so, give an attack in Alice-Bob Notation. If not, explain why. **[5 marks]**

3. (a) What is cross-site scripting? **[4 marks]**

   (b) A website contains the following code which sends a message, user name and password to a server:

```
1c  <form action="message.php" method="get">
2c  <p>Message: <input type="text" name="message" /></p>
3c  <p>Username: <input type="text" name="user" /></p>
4c  <p>Password: <input type="text" name="pass" /></p>
5c  <p><input type="submit" /></p>
```

   and on the server the message.php page processes this data:

```
1s  <?php
2s  $user = $_REQUEST["user"];
3s  $pass = $_REQUEST["pass"];
4s  $message = $_REQUEST["message"];
5s  $result = mysqli_multi_query($con,"UPDATE messages SET
6s     message=".$message." WHERE user=".$user."");
7s  $row = mysqli_fetch_array($result);
8s  if (!empty($row)) {
9s     echo "Your message: ".$message." has been added";
10s }
11s ?>
```

   Describe four security weaknesses in this website, how they might be exploited and rank them in order of severity. **[8 marks]**

   (c) Provide fixes for the security weaknesses you have identified. **[8 marks]**

A30303 Introduction to Computer Security

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.