A30303

Calculators may be used in this examination but must not be used to store text. Calculators with the ability to store text should have thier memories deleted prior to the start of the examination.

UNIVERSITY OF BIRMINGHAM

School of Computer Science

First Year – UG Affiliate Computer Science/Software Engineering
First Year – UG Affiliate Electronic and Electrical Engineering
Second Year – BSc Computer Science
Second Year – MSci Computer Science
Second Year – MEng Computer Science/Software Engineering
Second Year - MSci Computer Science with Study Abroad
First Year – UG Affiliate Business
First Year – UG Affiliate Science without Borders Computer Science
Second Year – BSc Computer Science with Industrial Year
Second Year – MEng Computer Science/Software Engineering with Industrial Year
Second Year – BSc Artificial Intelligence and Computer Science with Industrial Year
Second Year – BSc Computer Science with Business Management with Industrial Year
Second Year - MSci Computer Science with Industrial Year

06 26265

Introduction to Computer Security

Summer Examinations 2015

Time allowed: 1 hour 30 minutes

[Section A: Answer ALL Questions
Section B: Answer TWO out of THREE Questions]
[You will get an additional mark if you do NOT attempt to answer Three Questions]

Any Calculator

Section A

Answer all questions in this section. Write the question number and the answer letter on your answer paper, do not mark your answers on the exam paper. Each question is worth **3%**.

1. Which of the following are public key encryption schemes (write down all that apply):

   a) AES b) RSA c) DES d) Elgamal

2. Which of the following encryption schemes can be used for signing (write down all that apply):

   a) AES b) RSA c) DES d) Elgamal

3. If you want an RSA key to provide good security for at least the next 20 years what is the minimum length you should use:

   a) 512 b) 2048 c) 4096 d) 16384

4. Which mode of encryption provides authentication:

   a) CTR b) CBC c) ECB d) CCM

5. Which mode of encryption does not need padding:

   a) CTR b) CBC c) ECB d) RSA

6. Which mode of encryption is vulnerable to a known plaintext attack:

   a) CTR b) CBC c) ECB d) CCM

7. For which mode of encryption can an attacker recover the plaintext of messages if the same IV is used for every encryption:

   a) CTR b) CBC c) ECB d) CCM

8. Metasploit is a tool for:
   a) scanning machines on the Internet
   b) making and receiving Internet connections
   c) testing memory exploits
   d) proxying traffic

9. nmap is a tool for:
   a) scanning machines on the Internet
   b) making and receiving Internet connections
   c) testing memory exploits
   d) proxying traffic

10. netcat is a tool for:
    a) scanning machines on the Internet
    b) making and receiving Internet connections
    c) testing memory exploits
    d) proxying traffic

11. Which of the following is the credit card industry's security standard:

    a) PCI-DSS b) ISO27001 c) ISO7816 d) BSI-CardSec

Section B

Answer TWO out of three questions in this section, you will get 1 additional mark if you do not attempt to answer three questions. **[1%]**

1. (a) A website contains the following code which sends a message, username 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>
6c     </form>
   ....
```

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          $row = mysqli_fetch_array(mysqli_use_result($con));
 6s          if (!empty($row)) {
 7s              mysqli_multi_query($con,"UPDATE messages SET
 8s                 message='".$message."' WHERE user='".$user."'");
 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. **[16%]**

(b) Rewrite the lines of both pieces of code you would need to in order to fix the problems. Underline the fixes in your code, and briefly describe your fixes explaining why they fix the problems. **[11%]**

(c) Assume that all of the website is fixed and secure, give two examples of vulnerabilities that might still lead to the web server being compromised.

[6%]

2. (a) Consider the following C code, (`gets` reads a line from standard in and stores it into the string pointed to by its argument).

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

int main(int argc, char **argv)
{
  char buffer[64];
  gets(buffer);
}
```

Sketch the layout of the stack on an x86 machine immediately before the program reaches the `gets` command. Your diagram should clearly show the current top and bottom of the stack, the return address of the function, the arguments of the function and working space of the function.

[8%]

(b) Briefly explain what a buffer overflow attack is. **[2%]**

(c) Assume that code on the stack can be executed and that you can send code to the program via standard in. Explain how you could provide an input to this program to make it execute any command you wanted. Include in your answer a description of the input you would give it and the state of the stack during your attack (you may find it helpful to draw diagrams of these). **[11%]**

(d) Describe what a developer should do to defend against buffer overflow attacks **[6%]**

(e) Describe what steps a system administrator can take to defend their system against buffer overflow attacks. **[6%]**

3. (a) Alice wants to send the message "Transfer 10 pounds to Bob" to her bank. The Bank knows Alice's public key, and Alice knows the Bank's public key. To send her message to the bank Alice signs it with her private key, encrypts it with the bank's public key and then sends it over the Internet to the bank.

$$\text{Alice} \rightarrow \text{Bank} : E_{Bank}(Sign_{Alice}(Message))$$

Assuming that the encryption is unbreakable and that the keys are kept secure and they are not used for any other protocols, what security guarantees does this protocol provide to the bank?

[4%]

(b) Describe how an attacker could abuse this protocol.

[4%]

(c) What are the simplest additions you could make to this protocol that would ensure the secrecy, authenticity and freshness of the message in the protocol? Include your extended protocol in "Alice and Bob" notation and a description of how it works and why it provides these properties.

[12%]

(d) Assume that we have a server that has symmetric keys with Alice (K_{as}), Bob (K_{bs}) and Elvis (K_{es}). If Alice wants to set up a symmetric key with Bob she can run the following protocol:

$$\begin{array}{lll} \text{Alice} \rightarrow \text{Server} & : & A, B, N_A \\ \text{Server} \rightarrow \text{Alice} & : & \{K_{ab}, N_A, \{K_{ab}, A\}_{K_{bs}}\}_{K_{as}} \\ \text{Alice} \rightarrow \text{Bob} & : & \{K_{ab}, A\}_{K_{bs}} \end{array}$$

This protocol is not secure because Elvis can trick Alice into believing that he is Bob. Describe how, include the attack in "Alice and Bob" notation and a description of how it works and why it provides these properties.

[13%]