A28437

Calculators may be used in THIS Examination but must not be used to store text. Calculators with a ability to store text should have their memories deleted prior to the start of the examination

UNIVERSITY OF
BIRMINGHAM

School of Computer Science

MSc Advanced Computer Science
MSc Computer Security
MSc Robotics
First Year – UG Affiliate Science without Borders Computer Science
Fourth Year – MSci Computer Science
Fourth Year – MEng Computer Science/Software Engineering

06 23899

Computer Security

Summer Examinations 2015

Time allowed: 1 hour 30 minutes

[Answer THREE out of Four Questions

[Marks add up to 99%, an additional 1% will be added to your mark if you do NOT try to answer four Questions]]

1. Consider the following session:

```
>$ whoami
bob
>$ groups bob
bob : bob users
>$  ls -l
-rw------- 1 tpc  sysadmin  109 Feb 17 18:36 secret1
-rw------- 1 john sysadmin  109 Feb 17 18:36 secret2
-rwxr-sr-x 1 tpc  sysadmin 5418 Dec 20 10:03 execute1
-rwsr-x--- 1 tpc  sysadmin 5418 Dec 20 10:02 execute2
```

(a) Who can read the file secret1? **[2%]**

(b) Who can run the file `execute1` and what permissions does it run with? **[3%]**

(c) Assume that the execute programs will execute any command they are given as an argument, is it possible for bob to read the file secret1? Justify your answer. **[5%]**

(d) Given (c), is it possible for bob to read the file secret2? Justify your answer. **[5%]**

(e) Assume that Alice, Bob and Charlie are members of the group ABC and Alice, Bob and Elvis are members of the group ABE, is it possible for Alice to set the access control permissions on her files so that only she and Bob can read a file, without creating a new group? If so describe how. **[6%]**

(f) Is it possible for Alice to set the access control permissions on her files so that only she and Charlie can read a file, without creating a new group? If so describe how. **[6%]**

(g) If all of the access control settings on a system's files are correctly set how else could the files be accessed? **[6%]**

2. Consider the following website code:

```
<%
 ...
 function sanitizeSql($str)
 {
  $str = str_replace("%SELECT%", "_SELECT_",$str)
  $str = str_replace("%OR%", "OR",$str)
 }
 ...
 $action  = $_POST["action"];
 if ($action == "search" )
 {
   $query = sanitizeSql($_POST["q"]);
   mysqli_multi_query($con,"SELECT * FROM items
                                     WHERE name=’".$query."’");
   $row = mysqli_fetch_array(mysqli_use_result($con));
   echo "Item found";
 } else if ($action == "view_policy" )
 {
   $lang = sanitizeSql($_POST["lg"]);
   $sales_policy = readfile("policies/sales/"+lang);
   echo $sales_policy;
 } else if ($action == "email") {
   $to = $_POST["to"];
   $cmd = "bash -c cat invitation.txt | mail -s \"Invite\" $to";
   exec($cmd);
 } else {
   echo("action not found");
 }
 ...
%>
```

(a) This code contains three major vulnerabilities, explain what they are and where in the code they occur. **[9%]**

(b) For each of the vulnerabilities you identified write down a URL that an attacker could request from the website that would exploit the vulnerability. In each case explain what your exploit does. **[12%]**

(c) Suggests fixes for each of the vulnerabilities, give the code you would add to the website and say where it should be added, or where and what code should be removed. **[12%]**

3. (a) One of the important information assets owned by the School of Computer Science are the exam papers that are going to be given to students. What do you consider to be the three biggest threats to this asset? Justify your answer. **[6%]**

   (b) What other information assets do you think the school might own? Name three, and for each of these describe two major threats against them. **[9%]**

   (c) Assume that the University uses an impact scale from 1 to 10, where 1 means no important effects, 3 is an event that causes a small financial loss or damages the School's reputation in the University, 7 means major financial loss and 10 would be an event that would mean that the school could no longer continue to function. Rate each of the threats you have given, in (a) and (b), and briefly justify your answer.

   [12%]

   (d) Considering just the exam papers, what controls would you suggest the school puts in place to protect these assets? Consider the whole lifecycle of the paper until it is given to the student in an exam. If you need to make assumptions about how the School or University functions, say what these are. **[6%]**

4. (a) Consider the following protocol:

$$\begin{array}{lll} 1. & A \rightarrow B: & \{SessionKey\}_{Kab} \\ 2. & B \rightarrow A: & N_B, \{N_B\}_{Kab}, \{Message\}_{SessionKey} \end{array}$$

Alice (A) and Bob (B) share the key K_{ab}. Assume this key is kept securely and the encryption is good. Alice starts a run of this protocol by generating a session key, encrypting this with the shared key, and sending this to Bob. To prove to Alice that the reply really came from Bob, Bob generates a nonce N_B and sends this both in the clear and encrypted to Alice.

Why should Alice believe that the message from Bob is fresh and not a message replayed by the attacker?

[4%]

(b) Does this protocol keep the message secret? If so explain why, if not give an attack against the protocol in Alice and Bob notation that lets an attacker learn the message and explain the attack. **[8%]**

(c) Consider the following protocol:

$$\begin{array}{lll} 1. & A \rightarrow B: & g^x \\ 2. & B \rightarrow A: & g^y \\ 3. & A \rightarrow B: & Sign_A(g^y) \\ 4. & B \rightarrow A: & Sign_B(g^x), \{message\}_{g^{xy}} \end{array}$$

In this protocol Alice and Bob know each other's public keys. They then use Diffie-Hellman to establish a session key and then sign their messages to try to avoid a man in the middle attack. Unfortunately this is not secure. Give an attack in Alice and Bob notation that lets an attacker learn the message and explain the attack.

[8%]

(d) Define the term "forward secrecy".

[3%]

(e) What are small changes you can make to the protocol in part (c) to make the protocol secure and provide forward secrecy.

[10%]