University of Glasgow

Friday 6 May 2016
9:30 am – 11:30 am

(Duration: 2 hours)

DEGREES of MSc, MSci, MEng, BEng, BSc, MA and MA (Social Sciences)

Cyber Security (M)

This exam is worth a total of 60 Marks

Answer All 6 Questions

The use of a calculator is not permitted in this examination

INSTRUCTIONS TO INVIGILATORS

Please collect all exam question papers and exam answer scripts and retain for school to collect. Candidates must not remove exam question papers.

Question 1

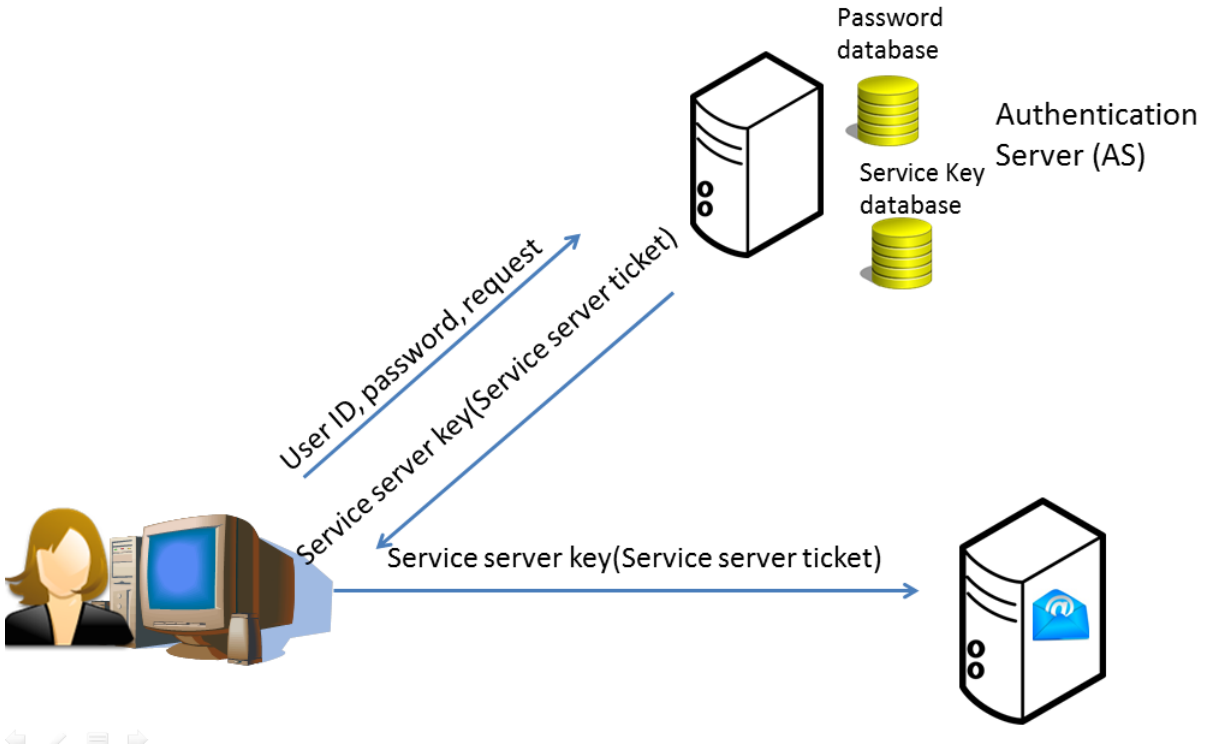

Figure 1

a) What type of network authentication protocol does the diagram in Figure 1 represent?

[2]

b) Briefly describe the type of attack is this protocol susceptible to.

[2]

c) How could you solve the attack described in (b)?

[3]

d) In the authentication protocol shown in Figure 1 Alice must send her password. How could you alter the exchange between Alice and the Authentication Server to remove the need for Alice to send her password, but still prove she is who she claims to the service server?

[3]

Question 2

Adams and Sasse wrote the seminal paper 'Users are not the Enemy'.

a) Provide a brief summary of what they did and the results of the paper. Your answer should be no longer than two paragraphs.

[5]

b) In your opinion, are users the enemy when it comes to computer security? Explain your answer in no more than two paragraphs.

[5]

Question 3

An authentication system for a store which performs repairs on computers and electronic devices has been proposed. The system will allow access to an application which manages orders. The database for the application contains personally identifiable information of the clients who have used the service, including payment information. The machines which access the database are located in the office at the back of the shop. The office is accessed by a locked door for which only staff has access. Staff are often called and asked to check up on the status of an order, this involves retrieving client data from the application quickly. Assume there are no limitations on cost.

a) What are the alternative factors which could be used to authenticate the users?

[3]

b) Which factor would be most appropriate for this scenario and why?

[3]

c) Given your choice of factor from b, which authentication system would you use and why?

[2]

d) The store management have decided to remove the lock from the door which permits access to the machine with the application installed on it. Occasionally staff are helping customers and it could be possible for someone to access the room with the machine in it. Would you change your answer to b)? Explain why.

[2]

Question 4

a) In public key cryptography, assume Alice receives a message encrypted with Bob's private key. What key would she use to decrypt this message?

[1]

b) In public key cryptography two keys are generated, knowing one key doesn't allow you to calculate the other. Explain why this is the case.

[2]

c) Provide an example of a public key cryptography scheme and highlight the way in which (b) is achieved for this scheme.

[3]

d) Describe how you can apply public key cryptography to prove integrity of a message

[4]

Question 5

A web application has been built for selling books for an online book store. The database for the web application contains book information, personally identifiable information about customers and order information. The books table has columns called title and author, both are of type VARCHAR.

One of the pages in the website contains a search field. In this field, the user can enter a title for a book to search for. If found, the application displays the details of that book to the user. The code excerpt below shows the book title being retrieved from the form field called "bookTitle". This code contains a vulnerability.

```
$book =$_POST["bookTitle"];

$query= mysql_query("SELECT title, author  FROM books WHERE title= '$book'
");

while($row=mysql_fetch_array($query,MYSQL_NUM))

{$result .= $row[0];}

if($result == '')

{echo "sorry, no books with that name exist";}

else

{echo $result;}
```

a) What attack is this vulnerability susceptible to? Indicate the line or lines which make the code vulnerable.

[2]

b) How you could exploit the vulnerability? Give an example of input and describe the expected output. You can assume there is a Users table with the columns username and password which are both type VARCHAR.

[3]

c) Describe how you could you fix the vulnerability.

[2]

d) The application developers have decided to hash the passwords in the database. They are choosing MD5 for their algorithm. Explain what makes a secure hash and why MD5 is a poor choice.

[3]

Question 6

A social engineer is trying to get access to a business's system. To achieve this, they wish to install malware on one of the machines on the network.

a) The social engineer first tries to achieve this by use of a phishing e-mail to one of the members of staff. This is shown in Figure 2. Identify the aspects of the e-mail which indicate it is phishing.

[3]

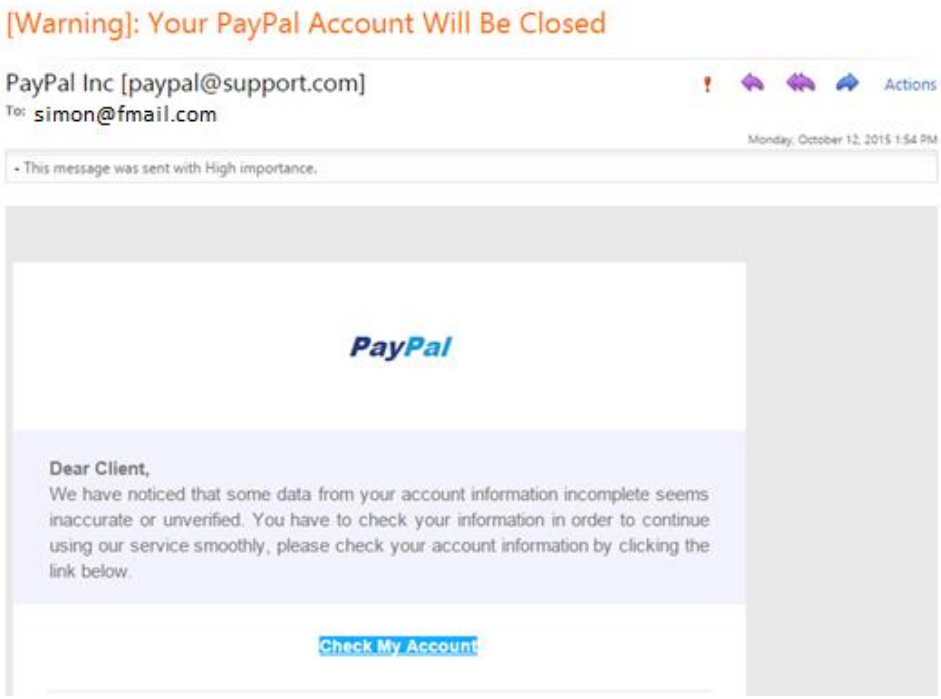

Figure 2

b) Assume that the malware in the phishing e-mail was purpose written by the attacker. Explain what antivirus approaches could be used to defend against the purpose written malware. Which would be most appropriate and why? Explain why you wouldn't use the other approaches.

[4]

c) The phishing e-mail did not work. The attacker decides on a more direct approach. They print pages of a presentation and cover it with coffee and dry it off. They then enter the company's main branch dressed as if for an interview. They approach the front desk and tell the receptionist that they are there for an interview and have spilled coffee on their presentation, they really need this job, could they please print out the presentation for them? Their interview is soon. The receptionist concedes and inserts the attackers USB which installs malware on the machine. Explain why this approach worked.

[3]