On admission to the examination room, you should acquaint yourself with the instructions below. You must listen carefully to all instructions given by the invigilators. You may read the question paper, but must not write anything until the invigilator informs you that you may start the examination.

You will be given five minutes at the end of the examination to complete the front of any answer books used.

May/June 2015 **SE3IS14 2014/15 A 001**

1 Answer Book
Only CASIO fx-83ES or -83MS calculators permitted

THE UNIVERSITY OF READING

INFORMATION SECURITY (SE3IS14)

Two hours

Answer any **THREE** out of FOUR questions.

EACH Question is 20 marks.

1. This question is about attacks and countermeasures.

(a) (i) What is SQL injection? (2 marks)

(ii) What can an attacker accomplish with SQL injection? (2 mark)

(iii) How can a system be hardened against SQL injection? (1 mark)

(b) Address Resolution Protocol (ARP) is a means by which IP addresses are assigned to devices. Assuming an attacker has full control over received and sent ARP packets on a networked machine, describe how that attacker could eavesdrop on network traffic. (5 marks)

(c) (i) Describe the differences between non-distributed and distributed denial of service attacks. (4 marks)

(ii) Describe a SYN-spoofing attack, and explain how it ties up resources in the target. You may use diagrams to illustrate your answer. (6 marks)

2. You work at a company that keeps all its server apparatus on-site and has thus invested a significant amount of time and effort into securing its web-facing services using measures such as firewalling, de-militarised zones and password and token based user authentication for offsite network access.

(a) How could an attacker totally bypass these protections and gain access to the company's internal network? (2 marks)

(b) Describe THREE network-based measures you (as the system administrator) could take to harden the company's internal network against attacks.

(6 marks)

(c) While performing a software audit, you find the following PHP snippet running on the company website.

```
<form action="authenticate.php" method="GET">
Username: <input type="text" name="user"><br>
Password: <input type="password" name="password"><br>
<input type="submit">
</form>
```

Explain the major security flaw in this code. (4 marks)

(d) Explain the principles behind a cross-site scripting attack in the context of an unsecured commenting system on a website.

Include the attack script in your answer with an appropriate payload. (8 marks)

3. (a) What is cryptographic concealment? (2 marks)

(b) What is the difference between stenography and cryptography? (2 marks)

(c) What is meant by a symmetric cryptographic algorithm? (2 marks)

(d) (i) Alvin and Beatrice wish to communicate securely, but have no way of meeting in person. Explain the process they could use to establish a secure channel using the RSA protocol. You may use diagrams to support your answer. (8 marks)

(ii) Is it feasible to use RSA for the entire communication? Justify your answer. (2 marks)

(e) Give a brief explanation of **TWO** actions that a malicious third party can take if they compromise Alvin and Beatrice's communication. (4 marks)

4. Information Security.

(a) The MD5 hashing algorithm has been proven to be vulnerable to collision attacks. Explain what is meant by a collision attack, and why this renders MD5 ineffective as a cryptographic hash. Provide an example. (6 marks)

(b) An attacker has stolen a table of passwords, stored as cryptographic hashes. Explain the principle of a lookup table extracting passwords from hashes. (4 marks)

(c) Explain how a rainbow table differs from a lookup table. (6 marks)

(d) Explain what could have been done to harden the password table against this attack. (4 marks)

(End of Question Paper)