UNIVERSITY OF SOUTHAMPTON COMP3201W1

SEMESTER 1 EXAMINATIONS 2014 - 2015

CYBERSECURITY

DURATION 120 MINS (2 Hours)

This paper contains five questions in three sections (A, B and C).

Answer **THREE** questions: the question in **Section A** (COMPULSORY) and **only ONE** question from **Section B** and **only ONE** question from **Section C**.

**Section A** carries 1/3 of the total marks for the exam paper and you should aim to spend about 40 minutes on it.

**Section B** carries 1/3 of the total marks for the exam paper and you should aim to spend about 40 minutes on it.

**Section C** carries 1/3 of the total marks for the exam paper and you should aim to spend about 40 minutes on it.

An outline marking scheme is shown in brackets to the right of each question.

A maximum of 99 marks are available for the paper.

Only University approved calculators may be used.

A foreign language translation dictionary (paper version) is permitted provided it contains no notes, additions or annotations.

## Section A

**A1.**

(a) Your company has discovered security vulnerabilities in a website that it operates. Senior management has assigned the task of securing the website to one of your colleagues, who, unfortunately, has no experience in this field.

Explain in detail each of the potential security threats below, including specific recommendations on how to modify the website server to remove each vulnerability:

(i) Broken authentication and session management;
(ii) Insecure direct object references;
(iii) Missing function-level access control;
(iv) Cross-site request forgery;
(v) Unvalidated redirects and forwards.

[17 marks]

(b) What other security vulnerabilities does your colleague need to be made aware of? Explain in detail *up to five* additional security threats, starting with the most important threat and then decreasing in importance. Justify the ordering of threat importance you have adopted, and in addition include notes on how to avoid each vulnerability.

[16 marks]

## Section B

**B2.** An ethical hacker has evaluated your security system and has been able to by-pass both your physical and electronic security systems to obtain company sensitive information. Your boss has asked you (the IT manager) for security improvements.

(a) Your system is currently using “username+password” to authenticate users. Describe in detail three alternative methods you could introduce to improve authentication.
[11 marks]

(b) Describe and explain the methods the ethical hacker could have employed to by-pass your security measures.
[11 marks]

(c) What is *digital forensic evidence*? Illustrate your answer by discussing examples of such evidence.
[11 marks]

**B3.** Your company has recently appointed you as systems manager and the Chief Information Officer has requested a review of the company security plan.

(a) With the aid of diagrams, explain and evaluate different possible *static security* models, including a full description and evaluation of a *“castle defence”*-like security model.
[11 marks]

(b) You company is using a *Discretionary Access Control* policy for its file store. Explain in detail how this works and assess whether it is appropriate for this application.
[11 marks]

(c) You notice that there is no risk analysis in the security plan. Why is it important to undertake a risk analysis?
[11 marks]

**TURN OVER**

## Section C

**C4.** The following monoalphabetic substitution cipher is used in this question to illustrate the different modes of use for block ciphers (note: “pt” = plaintext and “ct”= ciphertext) :

| | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 | 16 | 17 | 18 | 19 | 20 | 21 | 22 | 23 | 24 | 25 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| pt: | A | B | C | D | E | F | G | H | I | J | K | L | M | N | O | P | Q | R | S | T | U | V | W | X | Y | Z |
| ct: | Q | A | H | G | U | S | X | C | L | B | I | O | D | J | T | P | K | V | Y | E | W | R | M | F | Z | N |

(a) Explain in detail the advantages and disadvantages of the *electronic codebook* mode? Encrypt the plaintext “FIRST” using this mode and the cipher above.

[5 marks]

(b) Explain in detail the advantages and disadvantages of the *cipher block chaining* mode. Encrypt the plaintext “FIRST” using this mode and the cipher above. The exclusive-or operation is not defined for letters and should be replaced with the modulo 26 addition of the numerical plaintext equivalents (as given above). Use the initialization vector letter given by (your University registration number modulo 26). Every step of the encryption must be carefully explained.

[10 marks]

(c) What operation should replace the normal exclusive-or during cipher block chaining decryption? Decrypt the ciphertext “DRRERRI” using this mode and the cipher above. Every step of the decryption must be carefully explained.

. [12 marks]

(d) Propose three alternative strategies for the choice of an initialization vector. Evaluate your proposed strategies, explaining all of the advantages and disadvantages.

[6 marks]

**C5.** Your company operates a website that allows customers to login with a username and a password - both currently stored as plaintext files on the server. Senior management has assigned the task of improving password security on this website to one of your colleagues, who unfortunately has no prior experience in this area.

(a) Explain in detail *three* potential password attacks that are possible with the existing system.

[6 marks]

(b) Describe the concept of *password hashing* and explain in detail how the website system can be modified to incorporate such a scheme. Include in your answer a discussion and evaluation of any alternatives possible to the basic scheme, and also evaluate whether the possible attacks you identified previously still represent a serious threat.

[8 marks]

(b) Suggest and explain in detail another *five* possible improvements that could be introduced to enhance the security of the website password login system, and also evaluate whether the possible attacks you identified in (a) still represent a serious threat.

[8 marks]

(c) As an alternative to using passwords, customers could be provided with individual asymmetric-encryption key pairs (i.e. a private key with associated public key), which could be used to validate their identity on login. Design and explain in detail a suitable login system using asymmetric encryption, and evaluate any potential advantages and disadvantages of your proposed system.

[11 marks]

**END OF PAPER**