UNIVERSITY OF SOUTHAMPTON COMP3201W1

SEMESTER 1 EXAMINATIONS 2015/2016

CYBERSECURITY

Duration 120 mins (2 hours)

This paper contains six questions in two sections (A and B).

Answer **THREE** questions **ONLY**: **at least ONE** question from **Section A** and **at least ONE** question from **Section B**.

Each question 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 dictionary is permitted ONLY IF it is a paper version of a direct ‘Word to Word’ translation dictionary AND it contains no notes, additions or annotations.

6 page examination paper

SECTION A

Answer ONE or TWO questions only
(answer only ONE question in this section if TWO questions have been answered in Section B)

Question A1

You have just recruited a new systems programmer with little experience of security and need to discuss key issues.

(a) Explain in detail the threat of *spear phishing* (with examples) and discuss possible countermeasures.

[11 marks]

(b) Discuss in detail the alternatives to conventional “username+password” authentication, including the advantages and disadvantages of each alternative.

[11 marks]

(c) Explain in detail how a *Discretionary Access Control* policy operates, providing examples to illustrate how filestore access can be controlled.

[11 marks]

Question A2

You are the IT manager of a small company that has just been the victim of a cyberattack.

(a) Explain in detail the steps necessary to provide digital forensic evidence of the attack.

[11 marks]

(b) Describe in detail the steps necessary to restore your systems online.

[11 marks]

(c) Explain in detail possible improvements to increase the security of your systems.

[11 marks]

Question A3

You have just been appointed as the IT manager of a small company and are reviewing the security documentation.

(a) Explain in detail the function of a static security model and provide examples to illustrate your answer.

[11 marks]

(b) Explain in detail the different functions of a security policy and a security plan and discuss the expected contents.

[11 marks]

(c) Discuss the importance of undertaking a risk analysis and describe in detail the expected contents.

[11 marks]

TURN OVER

SECTION B

Answer ONE or TWO questions only
(answer only ONE question in this section if TWO questions have been answered in Section A)

Question B4

Collision resistance is an important requirement when a hash function is to be used in a digital signature scheme.

(a) Explain in detail the operation of a digital signature scheme and describe possible uses.

[8 marks]

(b) Explain exactly what is meant by *collision resistance*, why it is important for this application and discuss any other characteristics that the hash function should have.

[7 marks]

(c) Explain in detail how the AES block cipher can be used to construct a 128-bit hash function.

[10 marks]

(d) Provide a worked example of your answer to (c), replacing AES with a digit-by-digit modulo 10 encryption

$$\text{ciphertext} = (\text{key} * \text{plaintext}) \bmod 10$$

to produce a hash in the range 0 to 9.

Illustrate your example by hashing the numeric string 78942, explaining very carefully every assumption and step in your algorithm.

[8 marks]

Question B5

(a) Explain in detail how the *one-time pad* cipher operates, why it is resistant to cryptanalysis, the conditions necessary for secure communications and any advantages or disadvantages compared to alternative mechanisms.

[11 marks]

(b) The Advanced Encryption Standard (AES) defines operations on a 4-by-4 byte array (the ‘state’) with the following steps every round:

1. Substitution step (S-box)
2. Shift rows step
3. Mix columns step
4. Add round key step.

Assuming that the top row of the state is 0xB, 0xE, 0xE, 0xF (where the ‘0x’ prefix indicates hexadecimal), describe in detail the operation of a single round which results in the top row of the state being 0xD, 0xE, 0xA, 0xD (the intermediate results for every step of the algorithm must be included in your answer). All assumptions must be carefully explained.

You should omit step 3 above (the mix columns step) as no column information is available and assume that all bytes contain only values in the range 0 to 15. You will need to specify a suitable S-box and round key and explain how you have designed these (note that there is no requirement that your S-box be resistant to cryptanalysis).

[14 marks]

(c) Derive a suitable inverse S-box and demonstrate that the decryption of 0xD, 0xE, 0xA, 0xD results in 0xB, 0xE, 0xE, 0xF (again describing every step in detail and writing down the results at each stage of the algorithm).

[8 marks]

TURN OVER

Question B6

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, with specific examples of how to detect and exploit each vulnerability.

Include in your answer details and examples of possible PHP server code modifications to remove each vulnerability.

(a) Cross-site request forgery;
(b) Insecure direct object references;
(c) Cross-site scripting;
(d) Missing function-level access control;
(e) Unvalidated redirects and forwards;
(f) SQL injection;
(g) Sensitive data exposure;
(h) Broken authentication and session management.

[33 marks]

END OF PAPER