SEMESTER 1 EXAMINATIONS 2014 - 2015

IMPLEMENTING 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 is worth 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 existing experience in this field.

In particular, your colleague has become completely confused by the difference between *cross-site scripting* and *cross-site request forgery*. Write notes for your colleague explaining in detail the difference between these two vulnerabilities, the threat they represent and how each of them may be detected.

[11 marks]

(b) What other security vulnerabilities does your colleague need to be made aware of? Write introductory notes explaining in detail *up to six* 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 detect and avoid each vulnerability.

[22 marks]

A2.

(a) A *Caesar cipher* can be defined as follows:

ciphertext_symbol = (plaintext_symbol + key) modulo 26

where each symbol is a decimal number between 0 and 25. This cipher is applied to the following plaintext:

21, 4, 13, 8

using a key of 13, and the resulting ciphertext is then encrypted again, this time using a key of 16.

Discuss the advantages and disadvantages of this encryption system and calculate the intermediate ciphertext and final ciphertext (complete with a full explanation).

[7 marks]

(b) The double-encryption system described in (a) above is used with two 4-bit keys, K1 followed by K2. For a plaintext symbol of 17 the resulting ciphertext symbol (after the second encryption) is 16.

Calculate the keys K1 and K2 using a *meet-in-the-middle* attack, including a discussion of the advantages and disadvantages of this attack. All working must be clearly shown and explained (no credit will be awarded for any answer that does not use a meet-in-the-middle attack).

[13 marks]

(c) The cipher described in (a) above is a *stream cipher*. Explain in detail how a *block cipher* can be used to encrypt a stream of data values, discussing the advantages and disadvantages of using AES for such a system. Would an *asymmetric* block cipher be a suitable choice for such a system? Explain and justify your assessment.

[13 marks]

TURN OVER

A3.

(a) A security intrusion by a determined attacker will typically follow a sequence such as the one below:

(i) Initial compromise
(ii) Establish foothold
(iii) Escalate privileges
(iv) Internal reconnaissance
(v) Move laterally
(vi) Maintain presence
(vii) Complete mission

Write notes explaining in detail each of these activities.

[22 marks]

(b) Describe in detail the typical operation of a *firewall* and discuss the advantages and disadvantages in practice. Discuss the important issues faced by the systems manager of a company and propose how these may be addressed. You should include an assessment and evaluation of your proposals in your answer.

[11 marks]

Section B

B4.

(a) Explain the term *social engineering* and why it is important in cyber security. List and describe the main social engineering attacks.

[5 marks]

(b) Describe and discuss countermeasures to phishing attacks.

[7 marks]

(c) Explain why *passwords* are a significant practical problem in cyber security. Describe the main attacks against password systems and discuss the advantages and disadvantages of password alternatives.

[10 marks]

(d) What is a *trust and reputation system*, and how does it apply to cyber security? Describe some example trust and reputation systems to illustrate your answer.

[11 marks]

TURN OVER

B5.

(a) Explain the anonymity protocol *Crowds*. Use pseudo-code in your explanation rather than English prose.

[6 marks]

(b) Explain how *Tor* differs from *Crowds*. Pay particular attention to the notion of ‘onion’, its formation and decomposition, and to the creation of circuits (e.g. forwarding paths).

[7 marks]

(c) Explain and compare to each other the notions of *possible innocence*, *probable innocence* and *beyond suspicion*. Support your exposition with formulae (i.e. probabilities) which characterise these concepts.

[13 marks]

(d) Is *Tor* a better anonymity protocol than *Crowds*? Explain your answer informally. Does it provide superior anonymity *guarantees* than Crowds in terms of the notions mentioned in (c) above? Explain why.

[7 marks]

B6.

(a) Describe the major attacks to sensitive data, with particular reference to so-called *inference attacks* and the available countermeasures.

[8 marks]

(b) Describe and exemplify the concept of *privacy-preserving data mining* and the techniques it uses to preserve privacy.

[8 marks]

(c) Describe and exemplify the threats to privacy on the web.

[7 marks]

(d) What is *differential privacy*, what privacy goals does it focus on, and why it is a useful notion? Illustrate your answer with examples and mathematical details (where relevant).

[10 marks]

END OF PAPER