UNIVERSITY OF SOUTHAMPTON COMP6230W1

SEMESTER 1 EXAMINATIONS 2015/2016

IMPLEMENTING 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 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 question

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

(i) Broken authentication and session management;
(ii) Sensitive data exposure;
(iii) SQL injection;
(iv) Unvalidated redirects and forwards;
(v) Missing function-level access control;
(vi) Cross-site scripting;
(vii) Insecure direct object references;
(viii) Cross-site request forgery.

[24 marks]

(b) As an alternative to using passwords, your customers could each be provided with an individual asymmetric-encryption public-private key pair, 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.

[9 marks]

SECTION B

Answer ONE question only

Question B2

(a) Explain exactly the term *social engineering*. Describe *three* examples of the main attacks and their countermeasures.

[7 marks]

(b) State and explain *Dalenius' desiderata* for privacy in database systems. Is this an achievable aim? Explain your answer and illustrate with an example.

[7 marks]

(c) What is *differential privacy*? What privacy goals does it focus on? Why is it a useful notion? Illustrate your answer with examples and, if relevant, contrast with your answer to (b) above.

[10 marks]

(d) Provide an overview of *filesystem encryption* in Apple iOS. Illustrate your answer with a block diagram to show the components and their interactions. Extend your answer, to explain succinctly how the *data wipe* functionality is implemented.

[9 marks]

TURN OVER

Question B3

(a) What is *Tor* and what is it meant to achieve? Illustrate succinctly the way Tor works and describe its strengths and weaknesses in the contexts of some of its predecessors, such as *Mix networks* and *Crowds*.

[7 marks]

(b) What is intended by the term *attacker model* in the context of a network protocol? Describe and discuss the Tor attacker model.

[8 marks]

(c) Tor connects via TLS using 512-byte cells to avoid eavesdropping, impersonating and tampering. Describe the function and structure of both *control* and *relay* cells.

[9 marks]

(d) What is a *Tor circuit*? Use a communication chart diagram to illustrate the sequence of exchanges that Tor will use to create a *two-hop* circuit.

[9 marks]

SECTION C

Answer ONE question only

Question C4

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 its possible uses.

[8 marks]

(b) Explain exactly what is meant by *collision resistance* and why it is important for a digital signature. 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]

TURN OVER

Question C5

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 last digit of your University registration number to generate an initialization vector letter (use the mapping above). 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) Discuss three possible strategies for the choice of an initialization vector. Evaluate these strategies, explaining all of the advantages and disadvantages.

[6 marks]

END OF PAPER

