UNIVERSITY OF SOUTHAMPTON INFO6003W1

SEMESTER 1 EXAMINATION 2013 - 2014

APPLICATIONS OF SECURITY IN INFORMATION TECHNOLOGY

DURATION 120 MINS (2 Hours)

This paper contains 6 questions

Answer THREE questions, at least ONE question from each of Sections A and B.

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

Each question is worth 25 marks. The overall mark out of 75 will then be scaled up to 100.

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

Question A1.

(a) You own a copy of 'the essential student apprentice', a software package especially designed to assist students with their exam revision. This software has been copyrighted by the author and was sold to you under licence. You lend your copy to a fellow student, to help them with their exams. However, before returning the software to you, your friend makes their own copy of the package without your knowledge or permission. Explain the legal and ethical issues that are involved, discussing in detail all of the relevant points.

[11 marks]

(b) Attacks on computer system security are usually illegal. However, identification of the criminals responsible is often difficult. Explain why this is the case, discussing in detail all of the relevant issues involved.

[7 marks]

(c) Prosecution of the criminals responsible for attacks on computer system security is relatively uncommon. Explain why this is the case, discussing in detail all of the relevant issues involved.

[7 marks]

Question A2.

(a) Secure key distribution is an important security objective. To what extent does asymmetric encryption solve this problem? Your answer should include a full discussion of all relevant factors, including any advantages and disadvantages.

[8 marks]

(b) The Bank of Ponzi offers Internet banking to customers, but after repeatedly being hacked by foreign criminals it has decided to stop supporting user-generated passwords. Instead, customers will be provided with individual asymmetric-encryption key pairs (i.e. a private key with associated public key) to validate their identity on login. Explain in detail how such a system could operate and evaluate any potential advantages and disadvantages.

[9 marks]

(c) A stream cipher operates on a data stream of 8-bit characters using a simple monoalphabetic substitution technique. Estimate (and explain) the number of different substitution alphabets possible. Calculate (and explain) the effective key length of this cipher. Discuss the security of this system compared with AES, providing a full justification for your conclusions.

[8 marks]

TURN OVER

Question A3.

Botnets are formed when hosts are infected with malware and then accept and perform instructions from a command and control server.

(a) Explain in detail possible attacks that can be used to infect host nodes and discuss possible countermeasures.

[7 marks]

(b) Discuss in detail the various alternatives available for the botnet nodes to be controlled.

[6 marks]

(c) “Botnets can be hired out for phishing attacks.” Explain exactly what this means, with the aid of examples.

[6 marks]

(d) Another potential use for botnets is to launch Distributed Denial Of Service attacks. Explain exactly what this means and discuss in detail possible attacks that could be launched.

[6 marks]

Section B

Question B1.

(a) Explain the anonymity protocol `Crowds`. Use pseudo-code rather than English prose.

[5 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).

[5 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.

[10 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 at the previous point? Explain why.

[5 marks]

TURN OVER

Question B2.

(a) State and explain the *Dalenius' desiderata* for privacy in database systems. Is it an achievable aim? Explain your answer and illustrate it with an example, if relevant.

[5 marks]

(b) What is '*differential privacy*,' what privacy goals does it focus on, and why it is a useful notion? Illustrate your answer with examples and, if relevant, contrast it with your answer to the previous point.

[5 marks]

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

[9 marks]

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

[6 marks]

Question B3.

The Bitcoin is the best known, most successful and diffused crypto-currency in existence.

(a) Explain why Bitcoin transactions need to be verified, and how the Bitcoin system achieves that. You may find it useful to make reference to the notion of *blockchain*, why and how it is built and kept consistent, and how it achieves its purpose.

[10 marks]

(b) What are the deficiencies of the *proof-of-work* concept as implemented in the Bitcoin system? If so, explain which and discuss potential remedial and/or alternatives.

[5 marks]

(c) What are the main risks to user security, privacy and anonymity in the Bitcoin system? Describe and illustrate potential attacks and known countermeasures.

[10 marks]

END OF PAPER