UNIVERSITY OF SOUTHAMPTON INFO6003W1

SEMESTER 1 EXAMINATION 2012 - 2013

APPLICATIONS OF SECURITY IN INFORMATION TECHNOLOGY

DURATION 120 MINS (2 Hours)

This paper contains 6 questions

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

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

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 are the network manager for a campus enterprise network. Describe the security threats that your network is most likely to face.

[12 marks]

(b) What measures would you recommend be deployed to mitigate against the threats you have identified above?

[12 marks]

(c) What are the potential risks to the university should it fall victim to a successful security attack?

[4 marks]

(d) At a high level, how should the university manage the risks you have identified above?

[5 marks]

Question A2.

(a) A Distributed Denial of Service (DDoS) attack occurs when an attacker uses multiple hosts to coordinate an attack on a victim server or network.

(i) What resources might such an attack try to consume?

[4 marks]

(ii) What is meant by an amplification attack? How might an attacker use the DNS to launch such an attack?

[4 marks]

(iii) Suggest a measure that can prevent amplification attacks that use DNS, and explain how it mitigates the threat.

[7 marks]

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

(i) What command and control channels might a botnet use? Which do you think would be most effective?

[5 marks]

(ii) What messages or commands might typically be exchanged between an infected node and a command and control server?

[5 marks]

(c) "IPv6 vulnerabilities are not a security concern for sites that are IPv4-only." Discuss.

[8 marks]

TURN OVER

Section B

Question B1.

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

[9 marks]

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

[10 marks]

(d) Explain why the notion of *probable innocence* is being supplanted by quantitative approaches. Explain how you could use ideas from information theory (such as *entropy*) to express a measure of privacy.

[10 marks]

Question B2.

(a) List and describe the main security requirements of database systems.

[5 marks]

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

[9 marks]

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

[5 marks]

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

[5 marks]

(e) 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]

TURN OVER

Section C

Question C1.

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 tack of improving password security on this website to one of your colleagues, who unfortunately has no prior experience in this area.

(a) Write brief notes for your colleague explaining in detail potential password attacks that are possible with the existing system and explain how to modify the system to remove these threats.

[10 marks]

(b) Suggest and explain another five possible improvements that could be introduced to enhance the security of the passwords on the website.

[11 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. Explain in detail how such a system could operate and evaluate any potential advantages and disadvantages.

[12 marks]

Question C2.

(a) Explain what is meant by a brute-force known-plaintext attack on a cryptosystem. Estimate the average decryption time for 56-bit DES, explaining carefully all assumptions made about the computer system being used and also explaining all of the detailed steps in your working. Repeat this calculation for a triple-DES (3DES) system. Discuss and justify your conclusions about the security provided by these cryptosystems.

[9 marks]

(b) A stream cipher operates on a data stream of 6-bit characters using a simple mono-alphabetic substitution technique. Estimate and explain the number of different substitution alphabets possible. The key is effectively the substitution alphabet, which can be expressed as a 384-bit number (i.e. 64x6 bits). Discuss the security of this system compared with DES/3DES and a one-time pad, providing a full justification for your conclusions.

[12 marks]

(c) Explain what is meant by the key distribution problem, why it is an important factor in limiting the security that can be economically provided and typical mechanisms that attempt to address the difficulty. Finally discuss this problem given an objective of providing 'perfect security', explaining and justifying your conclusions.

[12 marks]

END OF PAPER