University of St Andrews

DECEMBER 2019 EXAMINATION DIET

SCHOOL OF COMPUTER SCIENCE

MODULE CODE: **CS4203**

MODULE TITLE: Computer Security

EXAM DURATION: 2 hours

EXAM INSTRUCTIONS

(a) Answer **three** questions.

(b) Each question carries 20 marks.

(c) Answer questions in the script book.

(d) Please start a new page for each question

YOU MUST HAND IN THIS EXAM PAPER AT THE END OF THE EXAM.

DO NOT TURN OVER THIS EXAM PAPER UNTIL
YOU ARE INSTRUCTED TO DO SO.

1. **Network Security**

(a) Name two tools to determine open ports during penetration testing.

[1 mark]

(b) Intrusion Detection tools monitor data packets passing through network nodes. Write pseudo code, or real code from any tool you have used, to

(i) Detect any IP packets on your computer. [1 mark]

(ii) Send an *Alert* signal when a particular IP address is sending more than 100 packets per second. [2 marks]

(c) AI and IDS is a growing area of research focussing on algorithms for detecting malware. Briefly explain the current research and industry problems concerning real-time intrusion detection? [4 marks]

(d) You have been asked to set up and test a small office network including wifi, and an email and website server. What can you advise with respect to security for both the setup and the testing of the whole system? [6 marks]

(e) How does the Kerberos network protocol:

(i) Indicate that sender is talking to the expected receiver? [2 marks]

(ii) Indicate that a conversation is new? [2 marks]

(f) Briefly explain the purpose and usage of a Security Parameter Index.

[2 marks]

[Total marks 20]

2. **Secure Access Control**

(a) Briefly explain

(i) The nodes and information required in Public Key Infrastructure.

[2 marks]

(ii) Potential and actual failures in PKI. [2 marks]

(b) Discuss and explain how well Unix, or one of its variants, can implement the Chinese Wall security mode? [4 marks]

(c) In a hospital environment, medical doctors and consultants, nurses and some support staff, such as administrative staff, must all access data on patients.

(i) Discuss how you would separate out the medical information about a patient from the personal (administrative data) such as name, address, National Insurance number etc? [2 marks]

(ii) How would you separate out the roles of technical and administrative staff from the various levels of medical professionals? What access control mechanisms and models would you use and why? [2 marks]

(iii) Your system is extended to allow for General Practitioners (GPs) and their nursing staff from a local practice, such as Pipeland or Blackfriars in St Andrews, to access a hospital patient system, such as at Ninewells Hospital in Dundee or Kirkcaldy's Victoria Hospital.

What access control mechanisms, models and system controls would you insist upon to enable Dr. Sam Smith at Blackfriars practice to access student Jane Doe's files in Ninewells Hospital in Dundee.

[4 marks]

(iv) Create four test cases to analyse and evaluate your hospital access control system. Indicate the actors (personnel), their role, rights and the expected outcome. Two of the test cases should result in rejected accesses and two in legitimate accesses. [4 marks]

[Total marks 20]

3. **Applications & Systems**

(a) During a Man in The Middle (MITM) attack there are at least three generic types of attacks that can be underway. What are they? [2 marks]

(b) Briefly discuss how you could detect two different types of attack by monitoring network packets. [4 marks]

(c) Protocols often use SSL (TLS) to perform an authentication handshake before the underlying protocol is initiated, as in HTTPS. What are the problems with SSL/ TLS? [2 marks]

(d) You have been asked to risk assess a new automated financial payment machine for a national supermarket chain which has different mechanisms for paying for goods.

A new QR code is generated every 15 seconds on the customer's mobile phone when the associated application is opened. This app is already linked to the supermarket's bank account, and the QR code will be read by a scanner at the supermarket checkout to enable direct payment from the linked user's bank account.

Separately, a user can use their normal bank card to pay for their goods, with PIN entry or contactless if the amount of goods is less than £30.

Finally, a separate loyalty card or mobile application can be used to collect "points" which have a low monetary value. When £1 or more is reached in loyalty payments this can be used to part-pay the check-out bill.

(i) Draw the boundaries of the system including the user, bank, supermarket and different payment methods, including the loyalty points. Make a note of the functionality needed between the boundaries and the physical, networking and data passing requirements. [6 marks]

(ii) What assessment actions can you take? [6 marks]

[Total marks 20]

4. **User and Usage Security**

(a) What are the disadvantages of using loci-centric password entry systems? [2 marks]

(b) Briefly discuss the user-based issues and concerns with ATMs or other PIN entry systems. Would security be improved if the four character entry included lower case alphabetic characters? Discuss. [4 marks]

(c) Produce a SWOT analysis on the use of biometrics for improved usability when using a cash machine (an ATM). [6 marks]

(d) In a Social Network Analysis there are measures of strength of a network and metrics to define particular nodes as important. In detail, discuss two of these metrics or measures and indicate why they are important for security monitoring of a social network. [4 marks]

(e) Consider the problem of raising Privacy Awareness in Social Networks? Is automatic sanitization of data uploads the answer to protecting users? Discuss. [4 marks]

[Total marks 20]

***** END OF PAPER *****