University of St Andrews

DECEMBER 2021
8 HOUR TAKE HOME EXAM
SCHOOL OF COMPUTER SCIENCE

MODULE CODE:	**CS4203**
MODULE TITLE:	Computer Security
TIME TO HAND IN:	8 hours
EXAM INSTRUCTIONS	a. Answer all three questions. b. Each question carries 20 marks

This assessment consists of exam-style questions and you should answer as you would in an exam. As such, citations of sources are not expected, but your answers should be from your own memory and understanding and significant stretches of text should not be taken verbatim from sources. Any illustrations or diagrams you include should be original (hand or computer drawn). You may word-process your answers, or hand-write and scan them. In either case, please return your answers as a single PDF. If you handwrite, please make sure the pages are legible, the right way up and in the right order. Your submission should be your own unaided work. While you are encouraged to work with your peers to understand the content of the course while revising, once you have seen the questions you should avoid any further discussion until you have submitted your results. You must submit your completed assessment on MMS within 8 hours of you downloading the exam. Assuming you have revised the module contents beforehand, answering the questions should take no more than three hours.
Some question may have word limits. These will be stated at the start of the question (or part question) and may be mandatory or advisory.

Answers which exceed a **mandatory** word limit may be penalised at the rate of 5% of the available marks for being overlength and a further 5% for each 10% over the word limit. So if the limit on a 20 mark question was 1000 words, an answer of 1201 words would attract a 3 mark penalty.

An **advisory** word limit is a guide to the level of detail and amount of information expected in an answer. Longer answers may lose marks for including large amounts of irrelevant material, or for failing to state arguments clearly and concisely.

1. **General Vulnerabilities & Network Security**

(a) Draw a threat tree for potential vulnerabilities on the physical and informational flow to a delivery vehicle driver, such as a DPL, Post Office or Hermes driver, who is attempting to deliver an item to yourself.

[4 marks]

(b) IPSec includes key and packet management to enhance communication security. Briefly explain the differences between the tunnel and transport IPSec protocols and why they are needed. [3 marks]

(c) Kerberos enhanced previous network protocols by introducing timestamps and liveness. Briefly explain these two terms and list problems or concerns using these parameters raises. [3 marks]

(d) Intrusion Detection is a major business need and much research has been done on AI and data analysis mechanisms as ways to make Intrusion Detection Systems (IDS) real time. Write a brief report for the owner of a start-up business to include the following:

(i) What is Intrusion Detection? Make especial mention of the two different main types. [4 marks]

(ii) Why is an intelligent approach to IDS needed? [3 marks]

(iii) Why is it unlikely that a recently installed IDS system will catch new abnormal traffic for several days, if not longer? What strategies could be employed to create a better training data set? [3 marks]

[Total marks 20]

2. **Confidentiality & Data Leakage**

(a) Briefly explain why hashing is used as well as encryption when a message is sent between a Sender and a Receiver. [2 marks]

(b) A cryptographic system has to be able to encrypt a message at the Sender end and decrypt at the Receiver end. Using a One Time Pad (OTP) a message can be hidden from eavesdroppers. Write pseudo code to describe the initial steps of generating a code book of characters, then choosing a random start position for a particular day and finally, passing that information to the Receiver. You can presume a library function for random character generation.

Note: Pseudo code can be a code like description of tasks or the necessary code statements can be written out in English if necessary. [3 marks]

(c) Briefly explain email vulnerabilities as outlined in the 2015 Baumgartner et al. and Durumeric et al. experimental papers on email security. Do you believe those vulnerabilities still apply? Give your reasons. [4 marks]

(d) Steganography can be used to leak information to a competitor. Briefly explain how an image can be adapted to hold information and, separately, how you would attempt to prevent this leakage vector. [3 marks]

(e) Using the ISO 27000 standard, or any other you are familiar with, briefly explain four types of risks, with two examples each for the following scenario:

A start-up company called Alpha has rented a small office in a tower block with dedicated space for small businesses. Alpha will offer financial services such as accountancy and tax filing and intend to build apps specific to a customer's business and financial needs. The tower block has key card access and a secondary PIN entry to identify users and allow access to the correct office. There is a Wi-Fi system enabled across the whole tower block which is offered to companies for a small fee and term, followed by a lock-in period. Some companies bring in their own Wi-Fi equipment. As you have some knowledge of security, you offer to advise them on potential vulnerabilities and risks via risk assessment.

[8 marks]

[Total marks 20]

3. **Supply Chain Security & Authentication**

(a) *You are a security officer hired by a European transportation company that moves expensive machinery parts, including computer parts, from various manufacturers in different countries, to different processing plants where the end products, such as laptops, routers or Wi-Fi access points, are built. The goods must then be packaged in the same processing plants. The packaged items are then distributed to large national warehouses and stored there until they are delivered to individual stores, including Amazon warehouses, for sale.*

(i) Draw a supply chain diagram to indicate the flow of goods and information from the initial manufacturing nodes through to the customers. [10 marks]

(ii) Briefly comment on six different security vulnerabilities from across the whole supply chain including at least one node (e.g. warehouse) and one arc (e.g. transportation). [6 marks]

(b) Perform a SWOT analysis on the use of fingerprint biometric authentication as a mechanism for paying for goods in a store, instead of using contactless card payments. [4 marks]

[Total marks 20]

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