

UNIVERSITY OF PORTSMOUTH

FACULTY OF TECHNOLOGY

Department of Electronic and Computer Engineering

M591 – Technology Exploration

U13127

Date: 29 January 2008

Time: 2 hours

INSTRUCTIONS

Write your student ID number clearly on page 2.

Write your answers to all 5 questions in this examination paper.

For each question, indicate your answer to **part A** by placing an “X” in the box next to the appropriate boxes on the answer sheet. For each question, write your answer to **part B** by writing in the appropriate space in this examination paper.

Handwritten notes are permitted with this examination.

Calculators permitted are:

Casio FX 85WA

Casio FX 83WA

Casio FX 85MS

Examiners:

Professor Zhili Sun, Mr Chi Nguyen

Student ID Number

Question 1A. Place an "X" in the box next to 3 terms that are most directly related to authentication claims. [6 marks]

X	statement		adversary
X	attribute		cover
	sensitivity	X	identifier
	threat		allocation
	integrity		initialization

Question 1B. Describe a specific example of a multi factor authentication system that uses all of the terms you selected in question 1A. Explain the primary purpose for using a multi factor authentication system. [14 marks]

Examples such as:

Application for a council resident parking permit requires multi factor authentication. I provide a written **statement** that I own the car that will use the permit. The council tax number verifies that I match the resident **attribute**. My driving license acts as a personal **identifier** with my application. (+10)

The primary purpose of using multi factor authentication is to increase the variety of failure modes so that there is less risk of having all the authentication modes fail at the same time. (+4)

Question 2A. Place an "X" in the box next to 3 terms that are most directly related to types of authentication infrastructure. [6 marks]

<input type="checkbox"/>	mutual	<input type="checkbox"/>	parallel
<input type="checkbox"/>	anonymous	X	decentralised
<input type="checkbox"/>	independent	<input type="checkbox"/>	complex
<input type="checkbox"/>	distributed	X	federated
X	centralised	<input type="checkbox"/>	reversible

Question 2B. Describe a specific example of an authentication system for each of the terms you selected in question 2A. Which of your examples would provide the best system performance? Which would provide the best privacy protection? Which would operate at the lowest cost? Provide a reason for each of your selections. [14 marks]

Examples such as:

Computer networks use **decentralised** authentication systems that are locally maintained, but interoperable on an as needed basis. (+2)

Driving licenses act as a **centralised** authentication system because it is primarily only usable within the country of issuance. (+2)

Passports operate as a **federated** authentication system because it is intended to be issued by one country and usable in other countries. (+2)

Decentralised computer network authentication provide the best performance because each network can use an authentication system that is most suitable for its user population and usage purposes. (+3) The same reason also leads to the lowest cost operations. (+2)

Passports provide the best privacy protection because there are strict controls regarding the exchange and use of personal data between countries. (+3)

Question 3A. Place an "X" in the box next to 3 terms that are most directly related to the use of patents. [6 marks]

<input type="checkbox"/>	advertisement	<input type="checkbox"/>	global
<input type="checkbox"/>	confidential	<input type="checkbox"/>	symbol
X	monopoly	<input type="checkbox"/>	article
<input type="checkbox"/>	secret	X	limited
<input type="checkbox"/>	image	X	utility

Question 3B. Use all of the terms you selected in question 3A to define patents. Describe two methods that a company could use to earn revenue from a patent without directly manufacturing tangible or physical products. Provide an example with each method. [14 marks]

A patent a **limited monopoly** for its owner regarding the production, use and sale of an invention. **Utility** patents are inventions that provide functional effects or benefits. (+4)

Instead of directly using the patent itself, a company could license the right to use that patent to other businesses. IBM receives many patents each year that it license to other companies. (+5)

A patent could be used to operate a commercial service. Amazon received a patent for its 1-click shopping cart that is used within the operations of its ecommerce websites. (+5)

Question 4A. Place an “X” in the box next to 3 terms that are most directly related to requirements of fair information principles and practices. [6 marks]

<input type="checkbox"/>	national	<input checked="" type="checkbox"/>	up to date
<input checked="" type="checkbox"/>	purposeful	<input type="checkbox"/>	database
<input type="checkbox"/>	anonymous	<input type="checkbox"/>	encoded
<input type="checkbox"/>	local	<input type="checkbox"/>	public access
<input type="checkbox"/>	inexpensive	<input checked="" type="checkbox"/>	accountable

Question 4B. Describe a fair information principle or practice that is relevant for each of the terms you selected in question 4A. Discuss how the Data Protection Act 1998 enforces the 3 principles and practices that you’ve described to improve personal privacy. [14 marks]

Personal data must be processed and used in a **purposeful** manner. (+2)

Personal data must be maintained so that it is accurate and **up to date**. (+2)

The organisation collecting personal data must be **accountable** for compliance with fair information principles and practices. (+2)

The Data Protection Act 1998 (DPA) enforces accountable behaviour through the requirement that any organization intending to collect personal data must register with the Information Commissioner (notification). (+3)

The DPA enforces purposeful usage of personal data by making compliance with fair information principles and practices a legal requirement. Failure to comply is a criminal offence. (+3)

The DPA enforces up to date maintenance of personal data through the requirement that notifications must be renewed annually by each registered Data Controller. (+2)

Question 5A. Place an "X" in the box next to 3 terms that are most directly related to examples of steganography. [6 marks]

X	null cipher	<input type="checkbox"/>	signature
<input type="checkbox"/>	hash value	<input type="checkbox"/>	random dots
X	invisible ink	<input type="checkbox"/>	binary grille
X	semagram	<input type="checkbox"/>	symmetric cipher
<input type="checkbox"/>	asymmetric cipher	<input type="checkbox"/>	message digest

Question 5B. For each term you selected in question 5A, indicate the type of steganography technique used and provide an advantage and disadvantage of that technique. [14 marks]

A **null cipher** uses the substitution technique. The advantage of this technique is that it has minimal change to the physical dimensions (e.g. weight) of the cover object. The disadvantage is that the quality or content of the cover object may degrade sufficiently to permit easier detection. (+5)

Invisible ink uses the injection technique. The advantage of this technique is speed because injection can often be done quickly or prepared ahead of time. The disadvantage is that the physical dimensions of the cover object may be altered sufficiently to permit easier detection. (+4)

A **semagram** uses the cover object creation technique. The advantage of this technique is ease of use because nearly anything can be created as a cover object for each secret message. The disadvantage is that semagrams are fragile and slight deformities to the stego object may render the semagram meaningless. (+5)