UOW AUSTRALIA

School of Computing and Information Technology

Student to complete:

Family name	
Other names	
Student number	
Table number	

CSCI262
System Security
Wollongong Campus

Examination Paper
Spring Session 2018

Exam duration	3 hours
Weighting	60%
Items permitted by examiner	Nil
Aids supplied	Nil
Directions to students	This exam contains three parts, for a total of 50 marks. Part A: 16 questions worth 1 mark each. Answer all questions. Part B: 7 questions worth 2 marks each. Answer all questions. Part C: 7 questions worth 4 marks each. Answer any 5 questions. Start each part on a new page.

This exam paper must not be removed from the exam venue

Part A: 16 questions worth 1 mark each. (Total 16 Marks)

For each of the following questions you should provide a brief solution to fill in the gap or gaps.
The size of gap does not generally indicate the size of an appropriate answer.
In cases where the answer could be an abbreviation you need to give the full name for full marks.
If you cannot think of a concise answer you can write more and still get full marks.

1) Examples of each of the main authentication bases are _____, _____ and _____.
2) A minimum time between password changes is specified so users _____.
3) Two security properties of a cryptographic hash function are _____ and _____.
4) "Online" and "offline" attacks differ in that _____.
5) A mechanism capable of distinguishing between humans and computers may be a _____.
6) Two primary properties used in malware classification are _____ and _____.
7) Two classes of intruder that an intrusion detection system may attempt to find are _____ and _____.
8) Race conditions can occur when _____ and can result in _____.
9) Phishing emails are typically sent in bulk because _____.
10) The Biba model is for the purpose of _____, while BLP is for the purpose of _____.
11) SYN flooding is an example of _____.
12) To be stateless means _____ and is relevant in the context of _____.
13) The term "shellcode" refers to _____ in the context of _____.
14) The difference between logging and auditing is _____.
15) A firewall cannot typically protect against _____ or _____.
16) The purpose of sanitization in the context of auditing is to _____.

Part B: 7 questions worth 2 marks each. (Total 14 Marks)

1) Describe two distinct types of attack against password systems and the countermeasures against each of those attacks.
2) Describe two general "good practices in coding". For each of them explain why they are appropriate and give an example of what could go wrong if that practice is not followed.
3) A company has two departments, A and B, and has determined that it is appropriate to have two levels of sensitivity, in increasing order: 0 and 1. Draw a BLP lattice system to represent this scenario. Using examples referring to this lattice, explain the three BLP rules, 2 mandatory and 1 discretionary.
4) Explain what tailored attacks are. Give some specific examples in two different domains and explain how they perform relative to other attacks in those domains.
5) Explain two outcomes an attacker may aim for with a Buffer overflow attack. Sketch how and why a Buffer overflow attack works. You do not need to write code but can if it helps you to explain.
6) Explain what a Trojan Horse is. Describe two distinct methods of identifying a Trojan Horse and explain when and why each of those methods might be appropriate.

7) What is a honeypot? What role might it play in the detection and management of intrusions? Give an example to illustrate how particular data within a real system might be considered to be a honeytoken.

Part C: 7 questions worth 4 marks each. (Total 20 Marks)

You are to answer FIVE of the SEVEN questions from this section.

1. The following questions relate to authentication:
   a. Explain how Unix protects user passwords. (**1 mark**)
   b. Which of the following two methods of generating a password is better? Justify your answer. In every instance the choosing is uniformly random. (**1 mark**)

      A: Choosing a seven digit number.

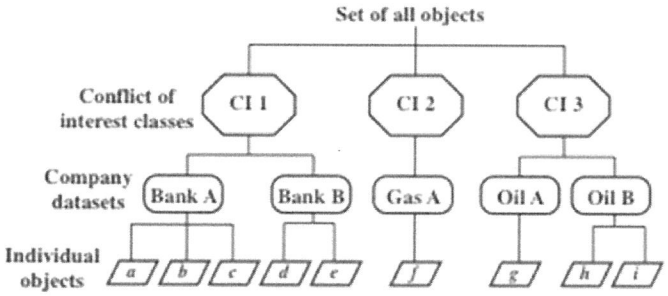
      B: Choosing a letter (upper or lower case), followed by three digits, followed by a lower case letter, followed by one digit then by the symbol #.
   c. Name and describe the two types of errors that occur in authentication systems. (**1 mark**)
   d. Sketch an example of an authentication scheme that utilises both two-factor and two-channel authentication. (**1 mark**)

2. The following questions relate to access control:
   Consider the following statements and answer the subsequent questions:

   Alice can climb trees and push walls.

   Bob can climb trees, push doors and jump fences.

   Chris can push Alice, open doors and climb walls.
   a. Draw an access control matrix for this scenario. (**1 mark**)
   b. Name the list representations corresponding to the access control matrix and give an example of each list representation. (**1 mark**)
   c. Use an example with appropriate subjects and objects to describe attribute-based access control. (**1 mark**)
   d. Name and describe the access control model related to the picture below. (**1 mark**)



3. One of the client puzzles we considered contained the statement h(C,Ns,Nc,Y) = 000…000X.
   a. Describe each of the components in the expression above? (**1 mark**)
   b. What is the purpose of using client puzzles? (**0.5 mark**)
   c. What is the chance of one guess succeeding in solving the puzzle, as an appropriate function of the difficulty? (**0.5 mark**)
   d. Explain what would differ if the right hand side of the statement was X000…000 rather than 000…000X? (**0.5 mark**)
   e. How do we typically solve such a puzzle? (**0.5 mark**)
   f. Describe how we could modify this to generate sub-puzzles. (**1 mark**)
4. Explain briefly what potential problem and domain each of the statements or code fragments is associated with, and what a likely effect would be. The syntax may not be precise.
   a. `Username: '; drop table users--` (**1 mark**)
   b. `strcpy(variable,"Polymorphic");` (**1 mark**)
   c. `srand(time())` (**1 mark**)
   d. `system(user_input);` (**1 mark**)

5. These questions relate to a variety of topics:
   a. In the labs for this subject various methods were used to unlock the exercises. Describe four of the methods used. (**2 marks**)
   b. What is the aim of inference in the context of statistical databases? (**1 mark**)
   c. Describe two methods than can be used to provide protection against statistical inference. (**1 mark**)

6. These questions relate to a variety of topics:
   a. Describe how virus and worm propagation differs. (**1 mark**)
   b. Describe a typical deceptive phishing process. (**1 mark**)
   c. Explain the role a sandbox might play in the detection and analysis of malware. (**1 mark**)
   d. Briefly describe how the three primary components of a virus are related. (**1 mark**)

7. These questions relate to a variety of topics:
   a. Describe positive and negative validation. Which is more appropriate? Why? (**1 mark**)
   b. Explain the difference between anomaly and signature based intrusion detection. Give an example to illustrate each. (**1 mark**)
   c. Explain what TOCTOU is. It is not enough to simply expand on the acronym. Give an example to assist in your explanation. (**1 mark**)
   d. CWE/SANS classify the top problems into three categories: Insecure interaction between components, risky resource management and porous defences. Name and briefly describe an example from each of these categories. (**1 mark**)

End of Examination