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 2017

Exam duration	3 hours
Items permitted by examiner	None
Aids supplied	None
Directions to students	This exam contains three parts, for a total of 50 marks. Part A: 15 questions worth 1 mark each for a total of 15 marks. Part B: 5 questions worth 2 marks each for a total of 10 marks. Part C: Answer 5 of the 7 questions for a total of 25 marks. Start each part on a new page. This paper is worth 60% of the total marks for the subject.

This exam paper must not be removed from the exam venue

Part A: 15 questions worth 1 mark each. (Total 15 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.
Where the answer could be an abbreviation you may 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) One type of malware that reproduces is ______________________________.

2) Inference is the derivation of ____________________ from ____________________.

3) The main advantage of using sub-puzzles in client puzzle systems is ____________________.

4) Password registration typically involves a user entering a password twice because ____________.

5) A mechanism capable of distinguishing between humans and computers may be a ____________.

6) Canary values are used to protect against ________________ by ________________.

7) The Biba mandatory rule is typically stated as ______________________________.

8) The principle of least privilege implies we should ______________________________.

9) To be stateless means ______________________________.

10) External traffic in a honeypot can **all** be usefully analysed because ____________________.

11) SYN flooding is an example of ______________________________.

12) The transaction property atomicity implies ______________________________.

13) Two types of activity we would expect to log in a computer system are __________ and __________.

14) DOS amplification is characterized by ______________________________.

15) The primary difference between software watermarks and software birthmarks is ____________.

Part B: 5 questions worth 2 marks each. (Total 10 Marks)

1) Sketch the typical process used in deceptive phishing. Explain how this differs from a pharming attack. Describe the relative use of technology and social engineering in deceptive phishing and in pharming.

2) Consider the following statements relating to access control in a scenario. Explain what subjects, objects, and actions are; and identify them for this scenario. Draw an access control matrix and give examples of the two list representations, carefully labelling them.

> **Alice eats apples, reads books, and opens doors.**
> **Bob eats bananas, reads magazines, and closes doors.**
> **Carol opens books, eats apples, and eats bananas.**

3) 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.

4) With reference to your third assignment, describe in detail the typical process of anomaly detection.

5) In the labs for this subject various methods were used to unlock the exercises. Describe four of the methods used.

Part C: 7 questions worth 5 marks each. (Total 25 Marks)

You are to answer FIVE of the SEVEN questions from this section. All questions answered will be marked and the best five will be counted. Note that answering additional questions will take up time that could be spent elsewhere.

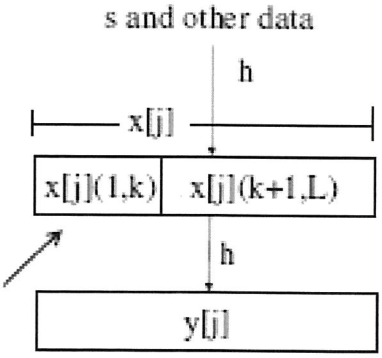
1. The following questions relate to auditing and intrusion detection systems.
   a. Describe one of the three "normal system behaviour" characteristics of Denning. Give an example to assist in your description. **(1.5 marks)**
   b. Explain the relevance of false positives and false negatives in the context of intrusion detection. Give an example of each. **(1.5 marks)**
   c. What is the purpose of log sanitisation and what does it involve? **(1 mark)**
   d. Give an example of a specific violation we might be attempting to find in auditing a BLP based system. Justify your answer. **(1 mark)**

2. The following questions relate to passwords.
   a. Assuming the attacker knows the method we use to choose a password, 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 six digit sequence.

      B: Choosing a lower case letter, followed by two digits, followed by an upper case letter, followed by two digits, followed by a $.
   b. Why could using the same password on multiple sites be a problem? **(0.5 mark)**
   c. What type of attack does a one-time password system attempt to protect against, and on what basis does it attempt to provide that protection? You need to explain the attack, not just name it. **(1.5 marks)**
   d. Why might we include a minimum time between password changes? **(1 mark)**
   e. Briefly explain the idea of rainbow tables and what they are used for. **(1 mark)**

3. The diagram to the right is associated with the client puzzle scheme of Juels and Brainard. The following questions relate to client puzzles.
   a. What are client puzzles used to protect against? **(0.5 mark)**
   b. On what basis do client puzzles provide that protection? **(0.5 mark)**
   c. Describe the meaning of L and the role of k. **(1 mark)**
   d. Give an example of what a single sub-puzzle might look like in the case k=4, L=8. **(0.5 mark)**
   e. For the case in part d, sketch how a client would go about solving the puzzle and explain what a solution would look like. **(1.5 marks)**
   f. For the case in part d, how much work would we expect a client to need to do? Justify your answer. **(0.5 mark)**
   g. Is the solution of the client unique? Justify your answer. **(0.5 mark)**



4. These questions relate to code security and secure coding.
    a. What does Raymond's modernisation of Kerchoff's principle state? (**1 mark**)
    b. What is the aim of digital rights management? (**1 mark**)
    c. Describe positive and negative validation. Which is more appropriate? Why? (**1.5 marks**)
    d. Sketch the process of a type-2 XSS attack and explain why these are also known as persistent XSS. (**1.5 marks**)

5. The following questions relate to malware:
    a. Describe how virus and worm propagation differs. (**1 mark**)
    b. Describe two methods we might use to detect a Trojan horse. Explain when each would be appropriate. (**1.5 marks**)
    c. What is a trigger in the context of a virus? (**0.5 mark**)
    d. What is ransomware and what does it attempt to do? (**1 mark**)
    e. Sketch how reducing the rights of a process can be used to protect against malware. Sketch an example. (**1 mark**)

6. The following questions cover a range of topics:
    a. Describe the idea of tailoring an attack. Give a specific example and explain why the chance of success is probably higher than for a generic attack. (**1.5 marks**)
    b. Part of your first assignment related to implementing a form of two factor authentication. Explain how such authentication works, both generally and in the example modelled in the assignment. (**1.5 marks**)
    c. Describe the differences between application-level gateways and packet filtering firewalls. What role is each likely to play in protecting a network? (**1.5 marks**)
    d. What is the DMZ with respect to firewalls? (**0.5 mark**)

7. The following questions cover a range of topics:
    a. A Biba based system is used in some Windows operating systems. What purpose does its use serve and why would a BLP based system be inappropriate? (**1 mark**)
    b. Describe two distinct scenarios or applications domains where we may use reverse engineering for legitimate and distinct purposes. Be sure to explain how reverse engineering may help.(**1.5 marks**)
    c. Explain how grouping can be used to simplify the representation of access control. Identify a grouping used in Question B.2, and explain how that helps. Describe two other types of grouping that may be used and sketch examples of each. (**2 marks**)
    d. How are master passwords and password masters related? (**0.5 mark**)

End of Examination