# CSCI262 – System Security (Wollongong Campus)

Sample Examination Paper

# Part A

1) Examples of each of the main authentication bases are _____ _____ _____ _____and_____ _____ _____

# Part A

2) Two security properties of a cryptographic hash function are _____ _____ and _____ _____

# Part A

3) “Online” and “offline” attacks differ in that

_____

_____

_____

_____

# Part A

4) Two possible consequences of a buffer overflow are _____

_____

_____ and _____

_____

_____

# Part A

5) The principle of least privilege is reflected via _____ _____ _____ _____ and _____ ___ in a lattice.

# Part A

7) Each row of the authorization table of Sandhu & Samarti contains _____
_____
_____
_____

# Part A

8) Two resources that can be targeted in a DOS attack are _____ and _____ _____ _____

# Part A

9) Random seeding a password generator with time alone is a bad idea because _____

_____

_____

_____

# Part A

10) Inference is the derivation of _____ _____ from _____ _____

# Part A

11) Spear phishing differs from general phishing in that

_____

_____

_____

# Part A

12) Error-based SQL injection uses _____

_____

_____

# Part A

13) An event being “Not known to be bad” likely refers to not being on a _____ _____ in the context of _____

# Part A

14) To be stateless means _____ _____ and is relevant in the context of _____

# Part A

15) A chain of custody provides assurances that

_____

_____

# Part A

16) Units are relevant in digital forensics and logging because _____

# Part B – Question 1 …1

1) Describe three distinct types of attacks against password systems. Briefly discuss appropriate countermeasures against one of those types of attacks.

# Part B – Question 2 ...1

2) Describe in detail how the one-time password system of Lamport works.

# Part B – Question 3

3) A company has three departments A, B and C, and has determined that it is appropriate to have two levels of sensitivity, in increasing order: L and H. Draw a BLP lattice system to represent this scenario.

# Part B – Question 4 …1

4) Explain what positive validation of user input is and why positive it is important, and usually more appropriate than negative validation of user input. You need to explain what is meant by positive validation and negative validation. Give examples to support your argument.

# Part B – Question 5

5) Pharming is considered to be more technical and social engineering than deceptive phishing. Explain how pharming and phishing are related and why this statement is reasonable. You should note both the technical and social engineering aspects of each.

# Part B – Question 6

6) Explain how the three classes of IDS attacker: clandestine, masquerade and misfeasor, differ from each other. Give example illustrating how the methods used to detect a masquerade might differ from those used to detect a misfeasor.

# Part B – Question 7

7) Describe factors used in differentiating between types of malware. Specify the main types of malware and illustrate how those factors apply to them.

# Part C – Question 1 ...

1. The following questions relate to authentication and access control:
   a. Explain what salting is, where we use it, and why we use it.
   b. 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.
      A. Choosing a six digit number.
      B. Choosing a lower case letter, followed by two digits, followed by an upper case letter, followed by two digits.

# Part C – Question 1 ...

c. Name and describe two list representations corresponding to an access control matrix. If we want to efficiently determine all the actions available to a subject, which of the two list representation is appropriate and why?
d. Name and describe the two types of error rates that occur in authentication systems.

# Part C – Question 1 …

a. Explain what salting is, where we use it, and why we use it.

# Part C – Question 1 ...

b. Constructing a password by choosing a seven digit number.

# Part C – Question 1 ...

B. Constructing a password by choosing a lower case letter, followed by two digits, followed by an upper case letter, and followed by two digits

# Part C – Question 1 …

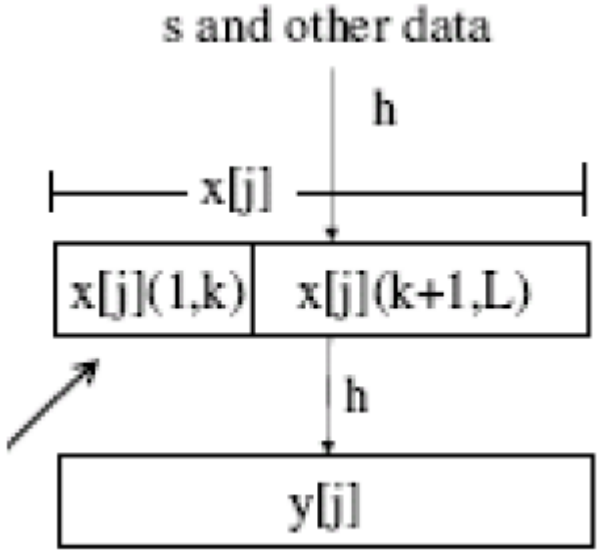
c. Name and describe two list representations corresponding to an access control matrix. If we want to efficiently determine all the actions available to a subject, which of the two list representation is appropriate and why?

# Part C – Question 7 …2

d. Name and describe the two type of error rates that occur in authentication systems.

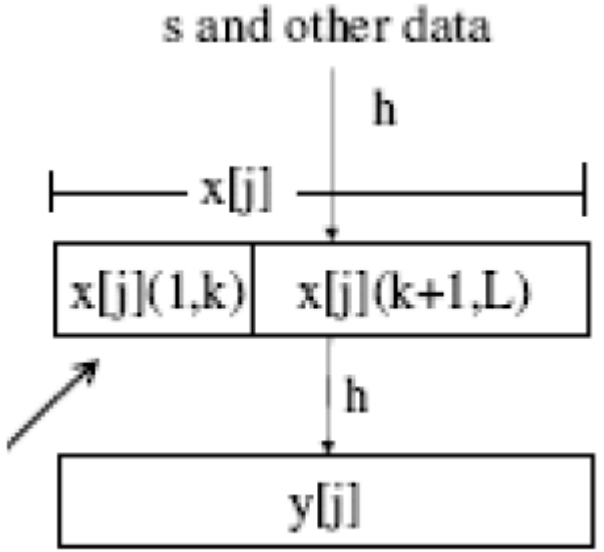
# Part C – Question 2 …1

2) Consider the diagram to the right and answer the following questions:
   a. What is the context of this diagram?
   b. What is sent to the client and how is this generated?
   c. What should the client respond with?
   d. What is the role of k?
   e. How much work would we expected the client to do?
   f. Is the answer from the client unique? Justify your answer.



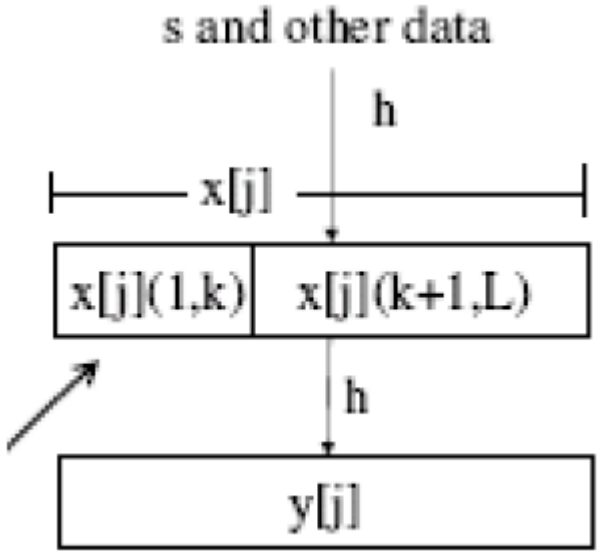
# Part C – Question 2 …2

a. What is the context of this diagram?



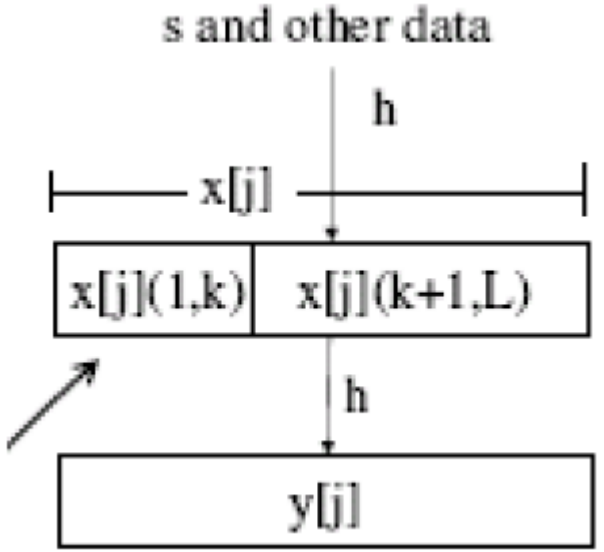
# Part C – Question 2 …3

b. What is sent to the client and how is this generated?



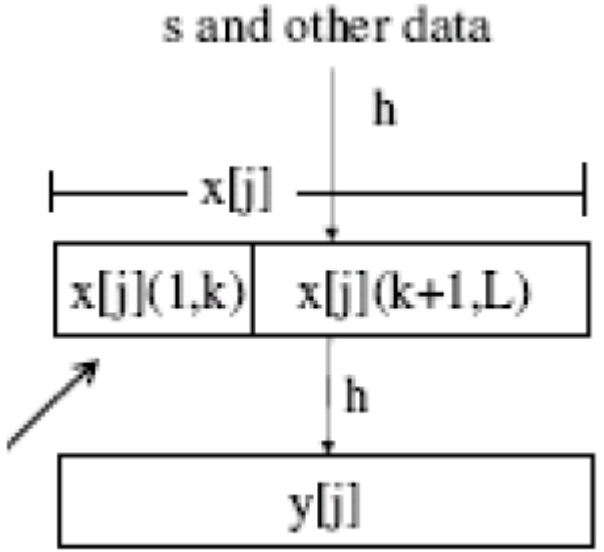
# Part C – Question 2 …4

c. What should the client respond with?



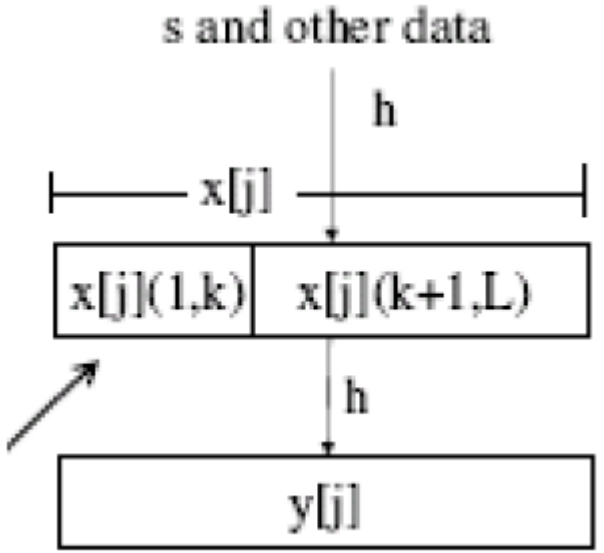
# Part C – Question 2 …5

d. What is the role of k?



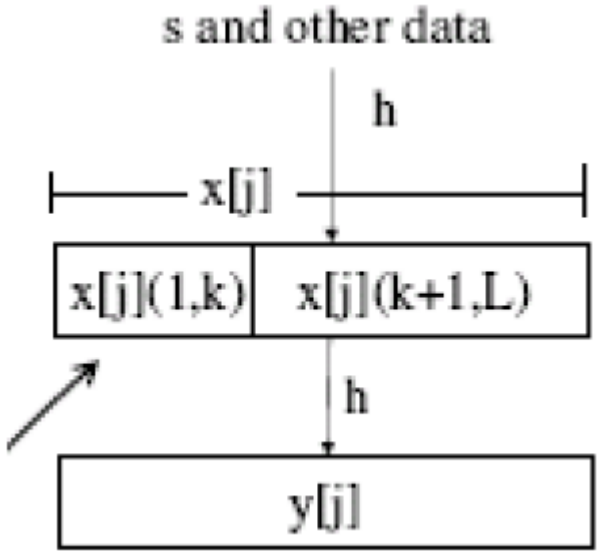
# Part C – Question 2 …6

e. How much work would we expected the client to do?



# Part C – Question 2 …7

f. Is this process stateless? Explain your answer.



# Part C – Question 3

3. The following questions relate to DoS attacks:
   a. What are the possible consequences or damages caused by a DoS attack?
   b. Describe the difference(s) between a quantity attack and a quality attack.
   c. Which DoS attack does Syncookie aim to resist? Briefly describe how Syncookie works.
   d. Describe 2 common techniques use by amplification attacks.

# Part C – Question 4

4. Explain what each of the following is/are, explaining the motivation and/or context for each as part of your answer:
   a. Master passwords
   b. CAPTCHA
   c. XSS
   d. TOCTOU

# Part C – Question 5

5. The following questions relate to intrusion detection:
    a. Explain the ideas of threshold models in the context of an intrusion detection system. Use a specific example to help in explaining.
    b. The lecture notes describe the 5+1 related goals of intrusion detection, the +1 being assurance. State and briefly describe the 5 goals. For each of those goals, give an example of what may happen if the goal is not met.
    c. What are honeypots? What role do they have in detecting and managing intrusions?

# Part C – Question 6

6. This is a collection of mixed questions.
    a. Describe what a timing side-channel attack is, illustrate how it might work, and describe a countermeasure to protect against such timing attacks.
    b. Describe a typical phishing process.
    c. What is Trojan Horse? Describe two distinct methods of identifying a Trojan Horse and explain when and why each of those methods might be appropriate.

# Part C – Question 7

7. This is a collection of mixed questions.
    a. Name and describe two methods of protecting, at the query level, against inferential attacks in statistical interfaces. For each of those methods describe a potential problem.
    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.
    c. A Biba based system is used in some Windows operating systems. What purpose does it’s use serve and why would a BLP based system be inappropriate?