CSCI262 – System Security (Wollongong Campus)

Sample Examination Paper

Part A

1) Examples of each of the main authentication bases are
_________________________, __________________________and
____
____
____
____
____
____.

Part A

2) CAPCHA can be used to provide protection against ______________________________

Part A

3) Obfuscation and reverse engineering are related in that ____

____

____

____

____

Part A

4) Two methods of grouping entities for access control are ______________________________________ ______________________ and ______________________________
____
____
____

Part A

5) A timing based side channel attack attempts to

____

_____________________ by ____________________

____

____

____

____

Part A

6) The use of external variables in languages such as PHP or Bash is dangerous because

____

____

____

____

Part A

7) Two things that packet filtering firewalls would typically filter based on are ___________________

and _______________________

Part A

8) SQL rand is a mechanism for ______________________

_____________________ by __________________________

____

____

____

Part A

9) A maximum time between password changes is specified so ____
____

Part A

10) The principle of least privilege implies we should

____

____

Part A

11) The Chinese Wall Model is designed to handle

____

____

____

____

____

____

____

Part A

12) Role hierarchies in RBAC support ___________________

____

____

____

____

Part A

13) The common ground between misfeasors and masqueraders is that both __________________________

____

Part A

14) Pharming involves ______________________________

____

____

____

Part A

15) DOS amplification is characterized by ______________

____

Part A

16) One advantage of using roles, in databases for example, is to ________________________________

____

____

Part A

17) To be stateless means ___________________________

_______________ and is relevant in the context of

____

Part A

18) Sub puzzles allow the average number of operations to ____________________ while ___________ the standard deviation.

Part B – Question 1

1) Explain what inference is in the context of statistical databases.
   Explain the difference between direct and indirect attacks, using appropriate examples.
   Describe one method of protecting against inferential attacks against statistical interfaces and a potential problem with that method.

Part B – Question 2

2) Explain why positive validation of user input is important, and usually more appropriate than negative validation of user input. Give examples to support your argument.

Part B – Question 3

3) Part of your first assignment related to implementing a form of two factor authentication. Explain how such authentication works, generally and in the example modelled in the assignment. Specify carefully the requirements of the “device”.

Part B – Question 4

4) There are various methods of protecting against denial of service attacks. Syncookies are a specific method while client puzzles describe a general protection methodology. Explain how syncookies and client puzzles are similar, and how they differ. Describe the main properties desirable for client puzzles. Use examples as appropriate.

Part B – Question 5

5) A company has two department, A and B, and has determined that it is appropriate to have three levels of sensitivity, in increasing order: X, Y and Z. Draw a BLP lattice system to represent this scenario. Using examples, explain the three BLP rules, 2 mandatory and 1 discretionary.

Part B – Question 6

6) In the third assignment for this subject you looked at detecting intrusions in an event based scenario. An example of the information your program was to initially generate was as follows:

Event	Average	Stdev	Weight
Logins	4.50	1.25	2
Total time online	287.15	42.12	1
Emails sent	65.40	30.71	1
Orders processed	150.73	20.13	1
Pizza’s ordered online	2.03	1.06	0.5

Part B – Question 6

6) Explain the ideas of threshold models and statistical models in the context of an intrusion detection system. Give a specific example of applying a threshold. Explain the idea of data aging in the context of the statistical models.

Part C – Question 1

1) For each of the following CWE’s, explain what the problem is and the potential “bad thing” that could happen.
   a. CWE-89: “Improper Neutralization of Special Elements used in an SQL Command”
   b. CWE-190: “Integer Overflow or Wraparound.”
   c. CWE-131: “Incorrect Calculation of Buffer Size.”
   d. CWE-306: “Missing Authentication for Critical Function.”
   e. CWE-807: “Reliance on Untrusted Inputs in a Security Decision.”

Part C – Question 2

2) The following questions cover a range of topics:
   a. 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.
   b. Describe the base rate fallacy problem. Explain where it is likely to occur, why it occurs, and what the potential effect is. Sketch an example to explain your answer. You do not need to give or use the formula in answering this question.
   c. Describe how virus and worm propagation differs.

Part C – Question 2

3) These questions relate to a variety of topics:
   a. What are honeypots? What role do they have in detecting and managing intrusions?
   b. What is XSS and what does it exploit?
   c. What are race conditions? Use an example to help your explanation
   d. What is a 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 3a

What are honeypots? What role do they have in detecting and managing intrusions?

Part C – Question 3b

What is XSS and what does it exploit?

Part C – Question 3c

What are race conditions? Use an example to help your explanation

Part C – Question 3c

What are race conditions? Use an example to help your explanation

Part C – Question 3d

What is a 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 4

4) The following questions relate to access control and authentication:

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

   b. Consider the following statements and answer the subsequent questions:

      Alice can jump fences and climb walls.

      Bob can paint fences, paint walls and roll barrels.

      Chris can climb walls and climb barrels.

      Dan can paint barrels and push Bob.

      i. What are the subjects, objects and actions for this scenario?

      ii. Draw an access control matrix for this scenario. Name and give an example of each of the list representations. Be sure to label all parts of your answer.

Part C – Question 4

c. 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 seven digit number.

   B. Choosing a lower case letter, followed by a digit, following by an upper case letter, followed by two digits.

Part C – Question 4

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

Part C – Question 4

b. Consider the following statements and answer the subsequent questions:

   Alice can jump fences and climb walls.

   Bob can paint fences, paint walls and roll barrels.

   Chris can climb walls and climb barrels.

   Dan can paint barrels and push Bob.

   i. What are the subjects, objects and actions for this scenario?

   ii. Draw an access control matrix for this scenario. Name and give an example of each of the list representations. Be sure to label all parts of your answer.

Part C – Question 4

c. 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 seven digit number.

   B. Choosing a lower case letter, followed by a digit, following by an upper case letter, followed by two digits.

Part C – Question 4

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

Part C – Question 4

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

Part C – Question 5

5) These questions relate to a variety of topics:

   a. Two versions of a loop are given below. One is an example of defensive programming. State which and explain why. You will need to briefly explain what defensive programming is to answer this question completely.

A

```
size_T elements = strlen(container);
for (i = 0; i < elements; ++i)
        state = combine(state, container[i]);
```

B

```
size_T elements = strlen(container);
for (i = 0; i != elements; ++i)
        state = combine(state, container[i]);
```

Part C – Question 5

b. Various Windows operating systems make use of a Biba-based system. Explain why it would be inappropriate for them to use BLP-based system for similar purposes?
c. What is the relevance of the return address in the context of buffer overflows?
d. Briefly explain the purpose of polymorphism in virus construction, using an example to illustrate what happens in polymorphic viruses.
e. How does a security audit trail differ from a security audit?

Part C – Question 6

6) These questions relate to a variety of topics.
   a. Describe one of the three “normal system behaviour” characteristics of Denning.
   b. Explain the relevance of false positives and false negatives in the context of intrusion detection. Give an example of each.
   c. Explain why each of the following rules might or might not be used in limiting password choices.
      I. A minimum length of password of 10 characters.
      II. Must be based on an uncommon dictionary word.
      III. At lease one alphabetical, one numerical and one special character.
      IV. Password changes every 50 days.
      V. Password changes no more than every 10 days.

Part C – Question 6

6) These questions relate to a variety of topics.
   a. Describe one of the three “normal system behaviour” characteristics of Denning.