CSCI262 – System Security (Wollongong Campus)

Examination Paper

Spring Session 2015

Part A

1) Examples of each of the main authentication bases are Single sign-on, multiple factor authentication and biometric.

Part A

2) CAPCHA can be used to provide protection against DOS (Denial of Services) attacks.

Part A

3) Obfuscation and reverse engineering are related in that reverse engineering is trying to produce the source code from the executable, but code obfuscation make it difficult to reverse engineer and obtain the code. In short, obfuscation is trying to prevent reverse engineering.

Part A

4) Two methods of grouping entities for access control are Group based access control, where users are assigned to groups and Role based access control (RBAC), where access control are done based on the roles that users assume in a system rather than the user's identity.

SIM-2016-S3-CSCI262-S3a, Slide 34, 37

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

PHP registers all kinds of external variables in the global namespace, hence there is really no way to ensure that those external variables contain authentic data that can be trusted. As a result, injection attacks are possible.

Part A

7) Two things that packet filtering firewalls would typically filter based on are Collection of rules and default security policy.

Part A

8) SQL rand is a mechanism for protecting a database against SQL injection by adding a random key to SQL keyword (internally). Before the keywords are actually sent to the database, the random key is removed.

Part A

9) A maximum time between password changes is specified so that user is forced to change his/her password.

Part A

10) The principle of least privilege implies we should give a subject the lowest security level to access a higher security level object.

Part A

11) The Chinese Wall Model is designed to handle conflict of interest, a concept that is used to control access to objects that might conflict the interest of the subject. The main idea in this concept is to use a logical wall (barrier) to prevent a subject that accesses data from one side of the wall from accessing data on the other side which has conflict of interest.

Part A

12) Role hierarchies in RBAC support hierarchical structure of roles in an organization. It makes use of the concept of inheritance to enable one role to implicitly include access rights associated with a subordinate role.

Part A

13) The common ground between misfeasors and masqueraders is that both have the password for a legitimate account.

Part A

14) Pharming involves modification of hosts file, perhaps through a virus, or by compromising or "poisoning" DNS servers that translate URL's into IP addresses.

Part A

15) DOS amplification is characterized by Making use of several intermediaries, e.g., zombies and reflectors.

Part A

16) One advantage of using roles, in databases for example, is to organize the granting of privileges base on least (minimal) required privileges by job scope or functional activities.

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 remain the same while reducing the standard deviation.

Part B – Question 1 …1

(SIM-2016-S3-CSCI262-S9b, slides 16 – 28)

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.

   Inference means the derivation of sensitive information from non-sensitive, typically aggregate, data.

   Direct attack is an attack where the aggregates are over small enough samples that information about individual elements of data can be obtained. Indirect attack is an attack where information external sources is combined with the results of aggregate queries.

Part B – Question 1 …2

An example of direct attack is an average salary of all employees older than 60 discloses an exact value of salary if exactly one employee older than 60 is employed.

An example of indirect attack is that we know, independent of the database, who lives in which suburb and who is a member of which department, the query …

```
SELECT SUM(SALARY), COUNT(*)
FROM EMPLOYEE
WHERE GROUP BY DEPTNAME, SUBURB;
```

… may then disclose the salaries of the employees who are the only people employed in a department and living in a particular suburb.

Part B – Question 1 …3

- One of the method of protecting inference attack is to design the database in such a way that inference is reduced. This approach removes an inference channel by altering the database structure or by changing the access control regime to prevent inference. One potential problem with this technique is the unnecessarily stricter access controls that may reduce availability.

Part B – Question 2 …1

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.

Positive validation concern a situation where we try to distinguish between authorized and unauthorized entities. A true positive and false positive may be the result of positive validation. A true positive refers to a situation when we make a match, and it is correct. A false positive refers to a situation when we make a match (a positive match) but which is actually not. Positive validation, in particular, a false positive, of user input is important because it affects the false acceptance rate.

Part B – Question 2 …2

A false acceptance rate is the proportion of authentication attempts resulting in false acceptances, which means the number of matches is accepted which we should not.

In a negative validation, of course there are true negative and false negative. A true negative refers to a situation when the match should be rejected and we did. A false negative, on the other hand, refers to a situation when we did not make a match, but we should have. A negative validation, in particular false negative, affects the false rejection rate, which means the number of matches is rejected which we should not.

Part B – Question 3 …1

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”.

Two-factor authentication implies the use of two independent means of evidence, such as a password or PIN and a device which is able to provide one-time type passwords, to assert an entity. This two-factor authentication system is based on smartcard technology and is successor to the old sign the imprint of the card type mechanism or swipe the magnetic stripe.

Part B – Question 3 …2

- The assignment simulates an authentication process using two factors. The first factor is the password, which is something one knows, and the second factor is the device, which is something one has. The authentication process works as follows:
  - To connect to a server, the server requests the user to present some evidence of his/her identity such as userid, and a one-time password that is generated by a device that the user has. (In the assignment, the device was simulated using a program.)
  - From the device, the user gets the one-time password and enters the one-time password together with a userid to complete the authentication.

Part B – Question 3 …3

- Upon receiving the one-time password and the userid from the user, the server will generate another one-time password based on the userid and the device id that was associated to the user. If this one-time password matches, the connection request is established, otherwise the connection request is rejected.

- The two-factor authentication seeks to decrease the probability that the requestor (in our example, the user) is presenting false evidence of its identity. For example, if the user does not possess the device, the user cannot generate the required one-password and hence the server cannot authenticate the user correctly.

Part B – Question 4 …1
(SIM-2016-S3-CSCI262-S4a, SIM-2016-S3-CSCI262-S4b)

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.

   Both are used as countermeasures to TCP SYN flooding attack. Syncookies avoid dropping connections when the SYN queue fills up. Severs uses a carefully constructed sequence number in the second message but discards the SYN queue entry. If the Server receives a “correct” ACK from the client, the Server can reconstruct the SYN queue entry and then connection proceeds as usual.

Part B – Question 4 …2

- As for the Juels and Brainard Client puzzles, puzzles will be presented when the Server detects a possible attack. When there is no evidence of a denial of service attack taking place, the Server accepts connections normally. However, when an attack on the Server is detected, perhaps through an intrusion detection system, the Server accepts connections selectively using puzzles.
- A client puzzle could be a cryptographic problem formulated using time and a server secret. The client needs to submit the correct solution to gain a connection. To be sure that very little work is required before the appropriate response is received, the generation of puzzle should not be too difficult and solving the puzzle should not be too tough either.

Part B – Question 4 …3

- One particularly important aspect of creating client puzzle is the flexibility and scalability. It is recommended that we treat the client puzzle as a number of independent sub-puzzles. The sub-puzzles may have different difficulties. With multiple sub-puzzles, we are able to maintain the total expected difficulty the same to that of a single puzzle and keep the standard deviation low.

Part B – Question 5 …1

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 …1

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 B – Question 6 …2

Statistical model for anomaly detection is where statistic of past data is used to detect the anomaly and threshold model which is the simplest statistical model is where an alarm is triggered if more than the certain number of something happened or less than the certain number of something is happened. An example is login event. If there is more than 5 login per day, an alarm may be raised. We should not heavily rely on old statistic. If we are accumulating data over a period of time and taking it all into account, we should weight the data as a function of time.

Part C – Question 1 …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 …1

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 …2

- Viruses infect files on the infected host, or in the boot area, to help aid replication.
- Worms replicate themselves to spread with minimal user interaction. Worms typically use widely available applications such as email to spread.

Part C – Question 2 …3

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 ...1

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

A *honey pot* is a decoy that lures attackers away from production systems. It's usually a computer attached to the network that runs special software to emulate services, applications, protocols. A honey pot should not contain any data other than the information specifically created to trick the attacker. Nor should it be allowed to connect to any other system except other honey pots, to prevent the attacker from using the honey pot to launch an attack.

Part C – Question 3a …2

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

We can use honeypots to rule the attacker to stay on the system long enough for the administrators to respond to the attack. In this case, the honeypots act as decoys in the intrusion detection and prevention system.

Part C – Question 3b …1

What is XSS and what does it exploit?

XSS is an abbreviation for cross site scripting. It exploits vulnerabilities in using dynamic web content, in particular, it involves the use of those vulnerabilities to gather data from a user that should not be gathered. XSS enables attackers to inject client-side scripts into web pages viewed by other users.

Part C – Question 3c …1

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

A race condition is a situation in which two or more threads or processes are reading or writing some shared data, and the final result depends on the timing of how the threads are scheduled. Race conditions can lead to unpredictable results and subtle program bugs. A thread can prevent this from happening by locking an object. When an object is locked by one thread and another thread tries to call a synchronized method on the same object, the second thread will block until the object is unlocked.

Part C – Question 3c …2

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

Classical example of Race condition is incrementing a counter. Incrementing a counter is not an atomic operation and can be further divided into three steps like read, update and write. If two threads try to increment count at a same time and if they read the same value because of interleaving of read operation of one thread to update operation of another thread, one count will be lost when one thread overwrite increment done by other thread.

Part C – Question 3d …1 (SIM-2016-S3-CSCI262-S6a)

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.

Trojan Horse are non-replicating program that openly exhibit one desirable behaviour, it might be a game for example, but have some real intent hidden from the user. This real intent could, for example, be to open ports on a machine to allow attackers access. A Trojan horse renames itself to the name of a valid system file. It can also be encrypted and polymorphic, and could install themselves in different ways to escape detection.

Part C – Question 3d …2

Two methods of detecting Trojan Horses:

- Monitoring – Make use of virus monitors to monitor known methods of virus activities, such as attempts to write to a boot sector, modify interrupt vectors, write to system files, etc. and detect abnormal behaviour of the system. This technique is able to detect the Trojan Horse before complete infection. The disadvantages is that to detect a high percentage of viruses, the sensitivity of the monitor must be set high and this may generate many false alarms.

Part C – Question 3d …2

Two methods of detecting Trojan Horses: (cont…)

- Signature scanning – the simplest and the most common approach to virus detection. With this technique, signature extraction is a non-trivial process. The infection is disassembled and the key portions are identified. Next, the key portions are combined to form a signature. The signature is then checked against a large library of programs to reduce the chance of false positives occurring when signature accidentally matches some library code. The advantage of this technique is that other than detecting Trojan Horse, it can also be used to detect logic bombs and other malicious software. The disadvantage is that scanning cannot find new viruses before their patterns are known. In addition, this technique is also ineffective against polymorphic viruses.

Part C – Question 4 ..1

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 ..2

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 ...3

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

One-time password refers to a password that can be used only for one session or one transaction. Lamport's one-time password is one example of such password. Lamport's one-time password consists of two parts, the setup and the process as follows:

Setup:

- In the setup process, a user is selecting a password that is secret to him/her.
- The system will then use this password, together with some value, say n, generate a sequence of passwords $p_1, p_2, \ldots p_n$.

Part C – Question 4 ...4

Process:

- A user, let's say Alice, request for connection to a server.
- The server issues a challenge n;
- The user responds with one-time password which is generated as $h^{n-1}(password)$
- The server checks if $h\left(h^{n-1}(password)\right) = h^{n}(password)$
- If it matches, then server accepts the communication request. If it does not, the server rejects the communication request.
- Once the user has been authenticated, the server needs to update its information.

Part C – Question 4 ...4

Process: (cont…)

- The system will then replace $x_n = h^n(password)$ with the one-time password sent by the user's, that is, $x_{n-1} = h^{n-1}(password)$.
- The value n is replaced by $n - 1$.
- When n reaches 0, the system will have run out of passwords in the hash chain and will have to run a new setup process, with a new base password.

Part C – Question 4 ...5

- Lamport's one-time password works because the system define p_i to be $H^{n-1}(p)$ where H is a hash function known to all, e.g., MD5() in our Assignment 1. In this way, attacker cannot derive future password from a past password. For example, after p_6, which is equals $H^{n-6}(p)$, the attacker can compute $H(p_6)$, which equals $H^{n-5}(p)$, the already used password p_5. The attacker cannot compute p_7 because p_7 equals $H^{n-7}(p)$, and computing $H^7(p)$ from $H^6(p)$ would require the attacker to computer the inverse of H or to know p, but H is a cryptographic hash function.

Part C – Question 4 ...6

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 ...7

Subject: Alice Bob Chris Dan

Object: Fence Wall Barrel Bob

Actions: Jump Climb Paint Roll push

Control Access Matrix:

Object / Subject	Fence	Wall	Barrel	Bob
Alice	Jump	Climb		
Bob	Paint	Paint	Roll	
Chris		Climb	Climb	
Dan			Paint	Push

Access Control List:

Fence: (Alice, jump), (Bob, paint)
Wall: (Alice, climb), (Bob, paint), (Chris, climb)
Barrel: (Bob, roll), (Chris, climb), (Dan, paint)
Bob: (Dan, push)

Part C – Question 4 ...8

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 ...9

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

$$Entropy = log_2 N^l$$

$$= log_2 10^7 = 7log_2 10 = 7 \times \frac{log_{10} 10}{log_{10} 2} = 23.25\ bits$$

$$Complexity\ of\ the\ password = \ 2^{23.25} \approx 9{,}975{,}792.32$$

Part C – Question 4 ...10

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

- One lower case letter: $26^1 = 26$
- One digit: $10^1 = 10$
- One upper case letter: $26^1 = 26$
- Two digits: $10^2 = 100$

$$Entropy$$

$$= 1 \times \frac{log_{10}(26 \times 10 \times 26 \times 100)}{log_{10}2}$$

$$= 1 \times \frac{log_{10}(676000)}{log_{10}2} = 19.37$$

$$Complexity\ of\ the\ password = \ 2^{19.37} \approx 677{,}565.08$$

Part C – Question 4 ...11

- From the previous computation, it is concluded that method one provide a stronger password. Although the second methods seem more complex, but because the pattern of creating a password is know to an attacker, this actually reduce the entropy of the password, and hence the complexity.

Part C – Question 5 …1

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 …2

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. (SIM-2016-S3-CSCI262-S6a, pg 41)
e. How does a security audit trail differ from a security audit? (SIM-2016S3-CSCI262-S8a,

Part C – Question 5 …3

- Program A is defensive programming. Defensive programming is to guard against unexpected errors, but defensive programming is different from error handling. If a public variable is to accept and store integer, and you check if the value is integer is error handling as we know beforehand. If a private variable is to accept and store an integer and a program function is used to store the value and check are in place to make sure it is integer is defensive programming. Program A is defensive programming as the for loop is checking for I < elements, and as long as this condition is satisfied, the loop will run and eventually terminate, but program B has I != elements. There is a possibility that I is larger than elements outside the code hence it will lead to an indefinite loop.

Part C – Question 6 …1

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.