Part B – Question 1 …1

1) Briefly explain the three basic components in an access control triplet. Describe how these triplets relate to an ACM. Give an example of an ACM, and the two related representations based on it, to illustrate your answer.

The three basic components of access control triplets are (S, O, A) where

- S: a set of subjects
- O: a set of objects
- A: an access control matrix, A[S, O] with entries a(s,o)

Part B – Question 1 …2

- A triplet describes the state and state transitions of an access control matrix (ACM).
- The following is one example of an access control matrix

Part B – Question 2 …1

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

- The three distinct attacks are dictionary attack, brute-force attack and hybrid attack. A dictionary attack uses a “dictionary” of all known words and try to find the password. Brute-force attack is trying all the possible combination of the password until it is correct. Hybrid attack is combination of brute-force and dictionary attack where we use dictionary as the basis but take variants on each of the words tested. We can protect against dictionary attack if we use words that are not commonly found in the dictionary or random words.

Part b – Question 3 …1

3) Consider a BLP lattice system with multilevel classifications $C = \{X, Y\}$ and multilateral categories $K = \{A, B\}$. Sketch a diagram to illustrate the relationship between the security levels in this system. Explain, with reference to your diagram, the concept of partial ordering. State the BLP rule and give an example, based on your diagram, to explain each aspect of it.

Part B – Question 4 …1

4) Describe the relevance of the Principle of Least Privilege in the context of Buffer Overflows. You will need to briefly explain the Principle and the possible relevant effects of Buffer Overflows, but not the details of Buffer Overflows themselves.

- Principle of least privilege in the context of buffer overflow is that we limit the access an attacker can have hence even if he identify a way to launch a buffer overflow attack. Effect of buffer overflow would be that the attacker may install a malicious code and then input the address of the code to the return address of the program, hence when the actual program returns, it actually runs the malicious code.

Part B – Question 5 …1

5) Briefly explain the difference between logging and auditing. Describe two specific considerations when determining what should be logged and audited, and explain how they may influence your decisions.

- Logging is recording of events or statistics to provide information of the system use, misuse and performance. Auditing is the analysis of the log events provided by logging and to provide the information of the system in a more readable and understandable manner. The two considerations are, we need to consider how the attempts that violate the security policies can be made and we need to consider how to detect those attempts. This may influence my decision as there is no point of detecting a problem if we do not know the indicating effect.

Part B – Question 6 …1

6) Garfinkel stated … "Something you had once, something you've…, or something ….". Complete the quote and explain the significance of it, in particular of this version.

Something you had once, something you have **known**, or something **you are**.

Part B – Question 7 … 1

7) Describe two general “good practices in coding”. For each of these explain why they are appropriate and give an example of what could go wrong if that practice is not followed.

The two general “good practices in coding” are:

- Never store secret in code
- Set default to deny instead of default to allow.

Part B – Question 1 …1

1) Describe the three main bases of authentication. Give an example of each. Describe an advantage and a disadvantage of each, either generally or for the specific example given.

The three main bases of authentication are:

- **Something you know**, e.g., password. Advantage of this base is a user can set his/her own desired password. The disadvantage is that password can be forgotten.
- **Something you have**, e.g., a “device” or key card. Advantage of this base is that authentication is easy. The disadvantage is the device may be lost.

Part B – Question 1 …2

- Something you are, e.g., fingerprint or any other biometric data. The advantage is this token cannot be lost or forgotten. The disadvantage is that the body part that is associated to the biometric information may be damaged, for example, finger may be accidentally cut (injured), and hence may affects the fingerprint.

Part B – Question 2 …1

2) Describe the use of access control matrices and how they relate to capabilities and access control lists. Give an example to illustrate your explanation.

Access control matrix is used to restrict subject from accessing objects that the subject is not authorized to act on.

Capabilities is from the perspective of subject, and access control list is from the perspective of objects.

Part B – Question 2 …2

Access control matrix:

	x	y	z	
Alice		rw	r	e
Bob		r	rw	

Access control list:

x : (Alice, rw), (Bob, r)

y: (Alice, r), (Bob, rw)

z: (Alice, x)

Capabilities:

Alice: (x, rw), (y, r), (z, e)

Bob: (x, r), (y, rw)

Part B – Question 3 …1

3) 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.

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 B – Question 3 ...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 B – Question 3 …3

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 B – Question 4 …1

4) Name and describe the two types of errors that occur in authentication systems and in intrusion detection systems. Give an example of each. Explain how the interpretation of each differs between authentication systems and intrusion detection systems.

Part B – Question 4 …2

False negative and false positive.

From authentication perspective, false negative and false positive concerns the likelihood of getting a result which is wrong, that is, an invalid user but falsely identify as valid (false negative) and a valid user but falsely identify as invalid (false positive). From intrusion detection perspective, false negative is when we do not make a match, but we should have, that is, there is an intrusion take place, but the system did not manage to identify/recognize it. A false positive is when make a match, but we should not have, that is, the system identify an intrusion, which is actually not.

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.

ss-property only can read below, *-property only can write up, ds-property – permission may be passed from an authorised person to a another, level authorized person

Part B – Question 6 …1

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 a 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 …2

Explain what each of these columns represent. How such values would be generated in practice, and how they are used in the detection of intrusions. You do not need to give numerical calculations but if it helps you to explain you can.

- The first column, “Event” contains the list of events being monitored.
- The second column, “Average” contains the average or mean that a particular event has under a normal situation.
- The third column, “Stdev” contains the standard deviation a particular events may be deviated from the mean. This can be the basis for specifying an anomaly, e.g., a measure as being more than a certain number of standard deviations away may be identified as anomaly.
- The fourth column, “weight” contains a factor to adjust the important or criticality of an event to the intrusions to be identified.

Part B – Question 7 …1

7) Explain what tailored attacks are. Give some specific examples in two different domains and explain how they perform relative to other attacks in those other domains.

Tailored phishing attack is where the attack is done on all people who are known to be customers to a particular banks etc. it is similar to tailored dictionary attack where we use what we know about the person to increase the likelihood of successful attack.

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 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.

- The three distinct attacks are dictionary attack, brute-force attack and hybrid attack. A dictionary attack uses a "dictionary" of all known words and try to find the password. Brute-force attack is trying all the possible combination of the password until it is correct. Hybrid attack is combination of brute-force and dictionary attack where we use dictionary as the basis but take variants on each of the words tested. We can protect against dictionary attack if we use words that are not commonly found in the dictionary or random words. Alternatively, use salt and regularly change the password.

SIM-2016-S3-CSCI262-S2a, Slide21

Part B – Question 2 ...1

2) 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 B – Question 2 …2

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 B – Question 2 ...3

Process: (cont...)

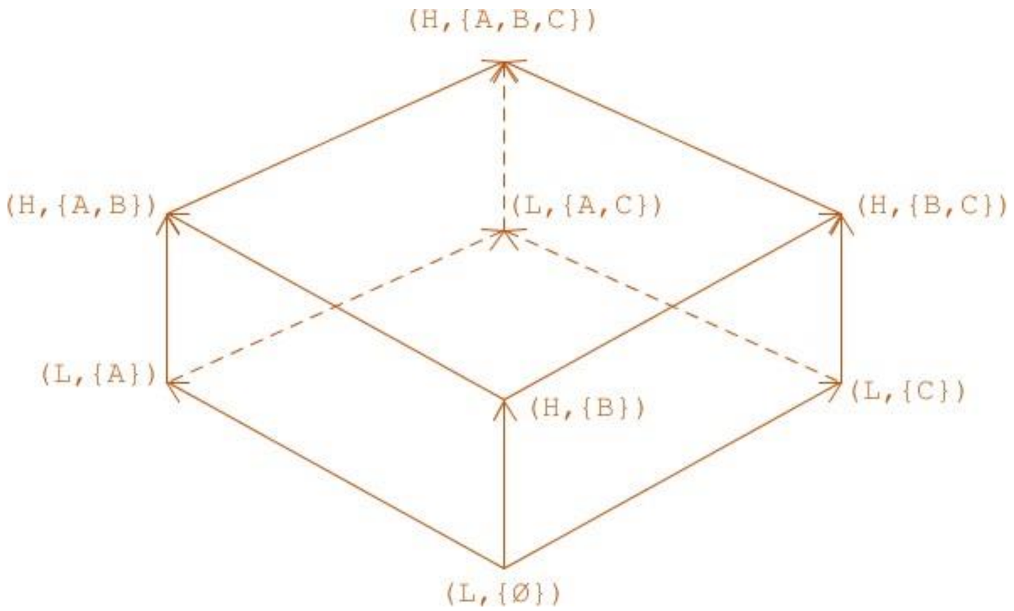
- The system will then replace $x_n = h^n\,(password)$ with the one-time password sent by the user's, that is, $x_{n-1} = h^{n-1}\,(password)$.
    - The value n is replaced by $n - 1$.
    - When n reaches 0, the system will have run out of passwords in the hash chain and will have to run a new setup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

Part B – Question 2 …4

- 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 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.

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 4 …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 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.

Masqueraders are those illegitimate users who are trying to imitate legitimate users while misfeasor are those authorized user who misuse their power.
Clandestine refers to someone who try to avoid the intrusion detection or auditing system.

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.