Examination Paper

Spring Session 2011

Part A

1) The phrase “Something you have, something you know, or something you are” refers to the bases of authentication. In authentication, something you have, something you know or something you are refers to the three factors use in authentication. An example of something you have is a staff card, something you know is a password, and something you are is a fingerprint.

Part A

2) Three types of malware are viruses , Trojan horses and worms .

Part A

3) Stack randomization is used to protect against ___ buffer overflow attack _____ and works by ____ randomizing the new buffer location, the new instance of the program run is probably in a different memory location and hence make the overflow attack difficult.

Part A

4) CAPTCHA can be used as protection against DOS (Denial of Services) attacks because bot (zombies) or automated system cannot read distorted image and hence this can be used to differentiate between a human (person) accessing system and a zombie accessing a system.

Part A

5) 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.

```
select gender, avg(age)
   from cs101.students
      where dept = %d
   group by gender
```


```
select123 gender, avg123 (age)
   from123 cs101.students
      where123 dept = %d
   group123 by123 gender
```

Part A

6) Salt is used in UNIX based password system, where the password and salt is hashed to hide the relationship between a user and the password used. In the event an intruder is able to get the password file, the intruder is not able establish the association of the password to its user because the salt is a value that is randomly generated.

Part A

7. XSS is an abbreviation for cross site scripting. It is a type of injection attacks in which an attacker can use to send a malicious script to an unsuspecting user and exploits vulnerabilities of dynamic web pages, in particular, it involves the use of those vulnerabilities to gather data from a user that should not be gathered.

Part A

8) Sanitisation in the context of logs involves removing information from the log that a user should not be able to see to provide confidentiality of the log.

Part A

9) Two classes of intruder that an intrusion detection system may attempt to find are: clandestine, who try to avoid the intrusion detection or auditing system and masquerader, who pretend to be a legitimate user.

Part A

10) Cohen's undecidability theorem states "It is undecidable whether an arbitrary program contains a computer virus."

Part A

11) A firewall cannot protect against internal attackers or services that by-pass the firewall, e.g., dial-up connection.

Part A

12) Single sign-on has a single point of entry as a gateway to multiple systems, using a master password, necessitating an equivalent number of sign-on dialogues, each of which may involve different usernames and authentication information.

Part A

13) A minimum time between password changes is specified so users are able (force) to change the password and to make sure that the passwords are secured from attacker who may be trying to hack their passwords .

Part A

14) The channels uses in two channel authentication are different between each other where one channel is between client and server, and the other is between server to client and must be independent.

Part A

15) Protection rings are an example of Role-base access control .

Part A

16) The BLP ds-property provides permission may be passed from an authorized subject to another, level authorized subject.

Part A

17) The two primary aims of digital forensics are to gather evidence from computer devices to investigate a crime or to recover lost data.

Part A

18) Pharming is more technical and less social engineering than deceptive phishing because it involves technology to perform the phishing act. It is carried out by modifying the hosts file through virus or “poison” DNS servers .

Part A

19) Consider that file A is infected with a virus, and that file B is not currently infected. File B can be directly infected by the actions of Carol if she executes file A and writes file B after that. By executing file A, Carol will be infected with the virus and by writing file B, the virus will be spread to infect file B .

Part A

20) An advantage of stateless puzzles over stateful puzzle is that the answer to stateless puzzle is nothing .

Part B – Question 1 …1

1) Describe why tailored, or spear, phishing attacks, and tailored dictionary attacks, are more effective than, respectively, general phishing or dictionary attacks. You will need to explain the idea of tailoring.

Tailored/spear phishing and tailored dictionary attack are more effective than general phishing. This is because, tailored phishing attack involves using what we know about somebody to increase the chances of the attack being successful while general phishing is total brute force which is inefficient compared to tailored phishing.

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 …1

3) Explain what inference and aggregated data are, and how one uses the other. Explain the context and describe how indirect attacks use something more than aggregate data.

Part B – Question 3 …2

Aggregate data is a single aggregated value over the column information and inference data are data which are derived using the aggregated data. Aggregate over a small sample leaks out information which is known as direct attacks. Indirect attack is where information from the external source is combined with the aggregate data.

Part B – Question 3 …3

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 4 …1

4) 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.

Part B – Question 4 …2

Logging is the recording of events or statistics to provide information about the system use, misuse and performance. Auditing is analysis of log records obtained by logging and present information about the system in a clear and understandable manner. The two considerations are, we need to consider how attempts to violate the security policies could be made and we need to consider how such attempts can be detected. It may influence many decision as there is no point detecting the problem if we do not know the indicating factors.

Part B – Question 5 …1

5) 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 5 …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 6 …1

6) What is a “sandbox environment”? What role do sandbox environments play in the security of mobile code, in the detection of malware and in honeypots?

Sandbox environment is a virtual environment which restrict sharing by controlling the domain boundaries. it plays an important role since if a software is suspected to be malware and it is affected, only that virtual environment vector is affected leaving the domain environment safe.

Part B – Question 7 …1

7) What are obfuscation and reverse engineering? Explain how they are related. Describe two simple transformations that could be used in obfuscation.

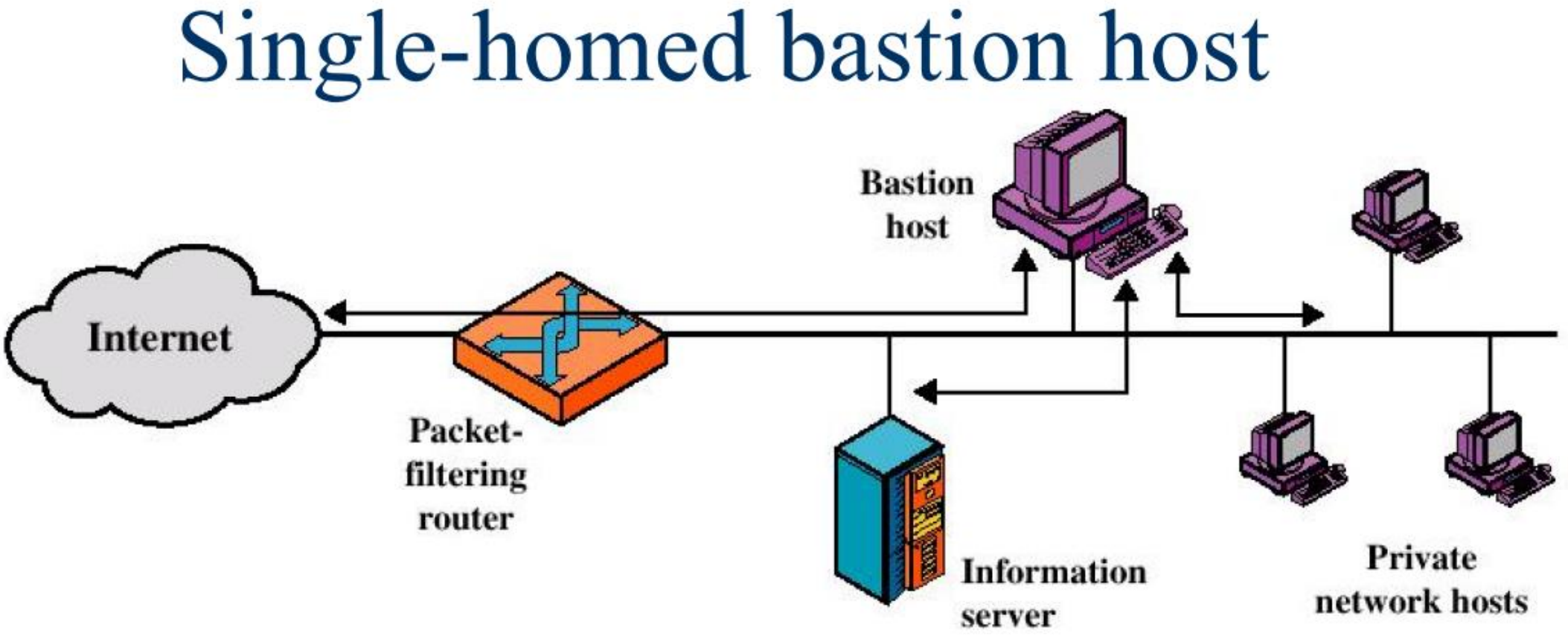
Reverse engineering is to take an executable and figuring out what is going on the inside or the design process and obfuscation in terms of code obfuscation is to encode/encrypt the source code so that it is not easily readable. They are related where reverse engineering is trying to produce the source code from the executable but code obfuscation make it difficult to reverse engineer and obtain the code.

Part B – Question 8 …1

8) What role does a bastion host play in firewall deployment? Sketch the model of a system containing a single-homed bastion host.

Bastion host are the host that the firewall administrator identifies as critical points in the security of the network. They usually have a limited functionality, to reduce exposure to weakness and improve performance and serve as a platform for an application-level gateway.

Part B – Question 8 …2



Part C – Question 1 …1

1) This question relates to access control models:
   a) State what BLP attempts to control, and the BLP policy.
   b) State what Biba attempts to control, and the Biba policy.
   c) The BLP and Biba rules are apparently very restrictive if applied together. Explain why. Explain how this apparent conflict can be resolved.
   d) If we have a lattice model with security levels (secret, {A,B}) and (secret, {B,C}) is it necessary for there to be a security level that dominates both? Justify your answer.

Part C – Question 1 …2

a) State what BLP attempts to control, and the BLP policy.

BLP attempts to control the confidentiality of the data. The BLP policy is no read up, and no write down, and the permission can be passed from an authorized person to another, level authorized person.

Part C – Question 1 …3

b) State what Biba attempts to control, and the Biba policy.

Biba attempts to control the integrity of data. The Biba policy is no read down and no write up.

Part C – Question 1 …4

c) The BLP and Biba rules are apparently very restrictive if applied together. Explain why. Explain how this apparent conflict can be resolved.

This is because BLP policy is used for confidentiality and Biba is used for integrity. When applied together some confidentiality properties are denied by Biba and some integrity properties are denied by BLP. We may revolve this conflict with the use of labels for both clearance and classification.

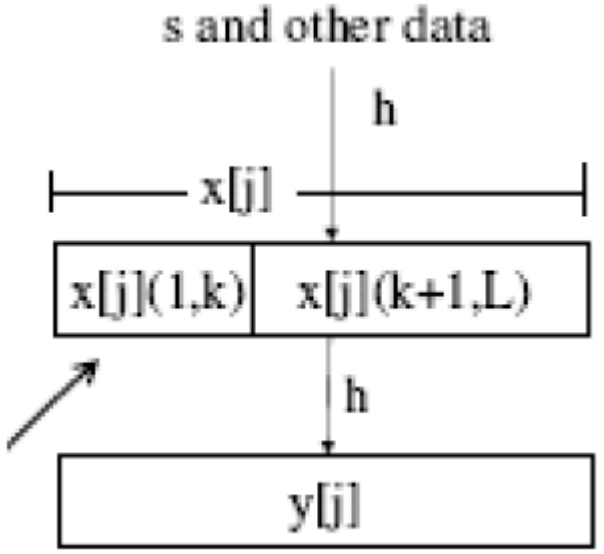
Part C – Question 1 …5

d) If we have a lattice model with security levels (secret, {A,B}) and (secret, {B,C}) is it necessary for there to be a security level that dominates both? Justify your answer.

Yes. For a lattice to be true, there needs to be a highest top level and lowest low level. the security level (secret,{A,B}) and (secret, {B,C}) is not the highest top level. Another dominating level for both is needed.

Part C – Question 2 …1

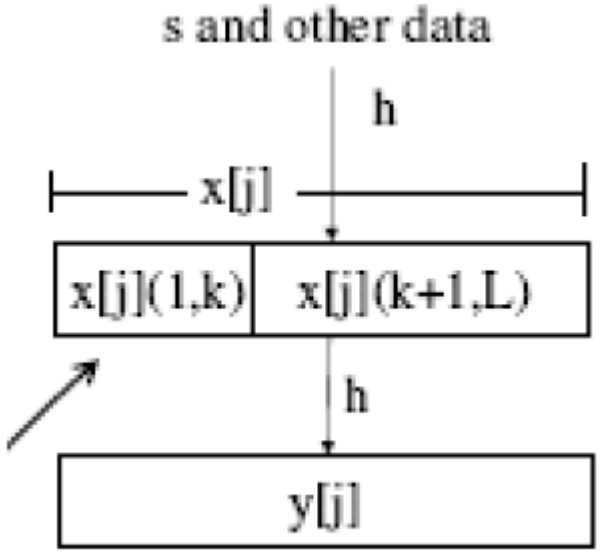
2) Consider the diagram to the right and answer the following questions:
   a. What is the context of this diagram?
   b. What is sent to the client and how is this generated?
   c. What should the client respond with?
   d. What is the role of k?
   e. How much work would we expected the client to do?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



Part C – Question 2 …2

a. What is the context of this diagram?

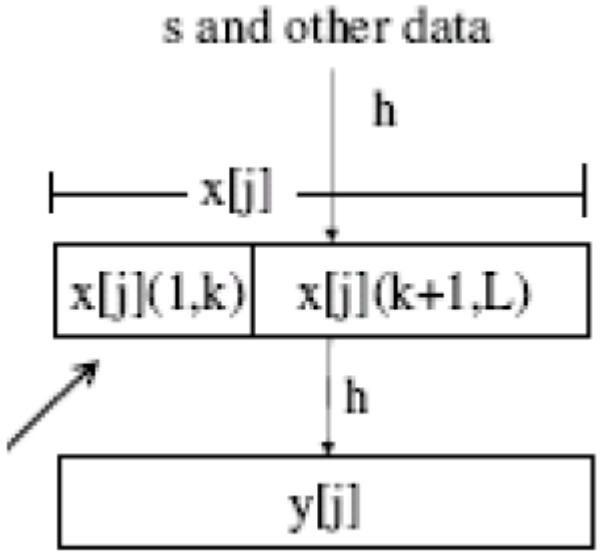
The diagram refers to the construction of client puzzles.



Part C – Question 2 …3

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

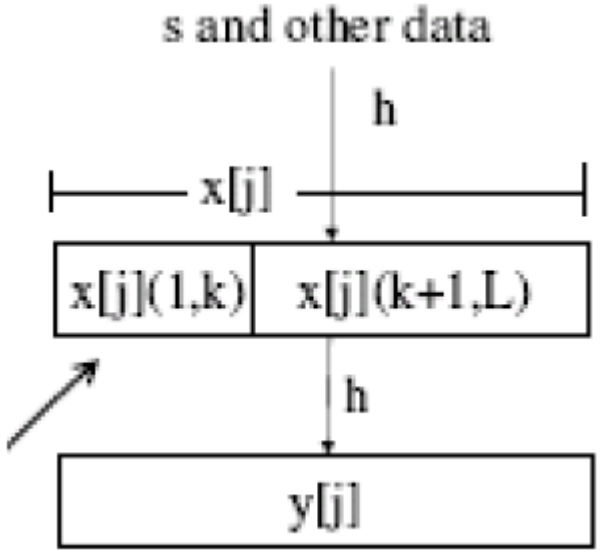
X[j](k+1,L) is sent to the client. This is generated by taking a sub-puzzle and taking k bit as the solution of the puzzle



Part C – Question 2 …4

c. What should the client respond with?

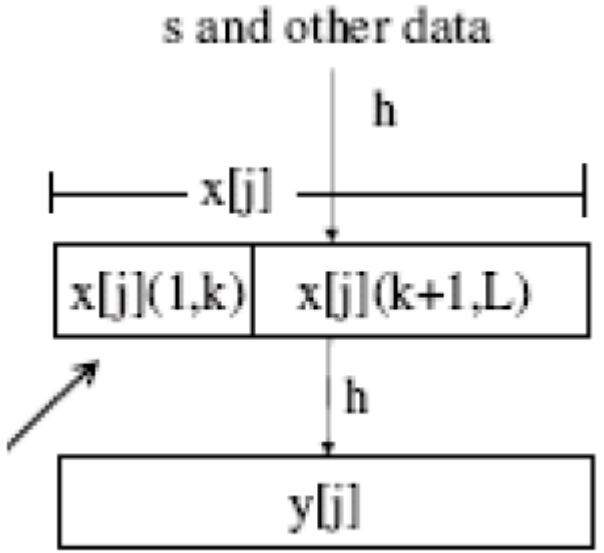
The client should respond with x[j](1,k) to be joined with x[j](k+1,L) to get y[j].



Part C – Question 2 …5

d. What is the role of k?

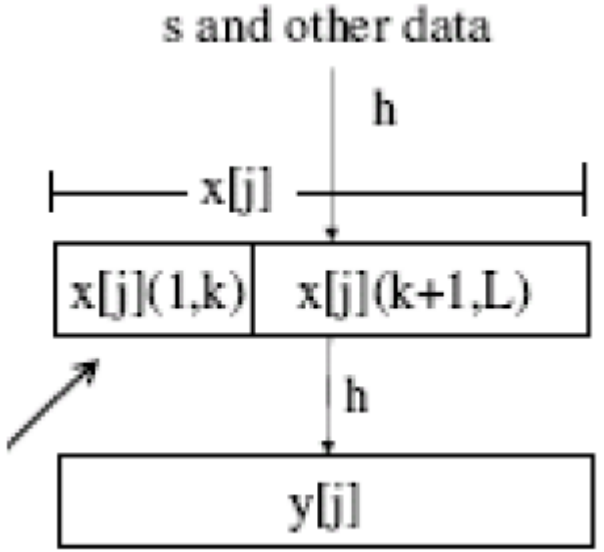
k is the number of bits that are missing from the puzzle. It determines the complexity (efforts) that a client needs to put in to solve the puzzle.



Part C – Question 2 …6

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

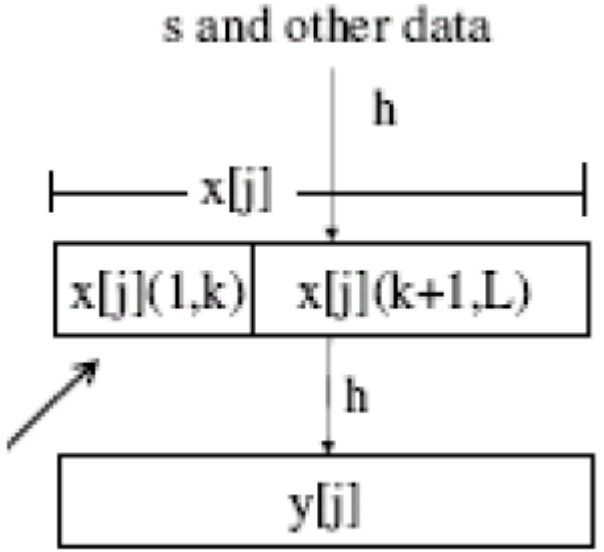
The client is expected to do minimal work so that the authentication can be fast.



Part C – Question 2 …7

f. Is this process stateless? Explain your answer.

Yes, the puzzle stores no information. The solution itself contains all the information the server needs other than their own server secret.



Part C – Question 3 …1

3) The following questions are all related to malware.
   a. Describe how virus and worm propagation differs.
   b. Explain how Trojan horses have overt and covert behaviours. Give examples.
   c. How do Oligomorphic, polymorphic and metamorphic viruses differ?
   d. Describe the difference between direct action and memory residence.

Part C – Question 3 …2

a. Describe how virus and worm propagation differs.

Virus propagates on the manual transfer of virus infected files while worm propagate using network connection.

Part C – Question 3 ...3

b. Explain how Trojan horses have overt and covert behaviours. Give examples.

Trojan horse overt behaviours are documented effects and covert behaviours are non-documented effects. Eg. overt – denial of service, covert is backdoor.

Part C – Question 3 ...4

c. How do Oligomorphic, polymorphic and metamorphic viruses differ?

Oligomorphic viruses change the decryption of the algorithm between generations. They carry a collection of decryption algorithm and deploy any one of them in any instance. Polymorphic viruses change form each time they are inserted into another program. They change the instruction of the virus into something equivalent but different. Metamorphic viruses are a higher order polymorphic viruses; not only they change form between transition, they can completely re-written.

Part C – Question 3 …5

a. Describe the difference between direct action and memory residence.

Viruses install themselves into the memory of the host computer when the original virus program is executed. Even when the original virus program is closed, new object can still be infected without having to run anything else. These are called memory residence. Direct action viruses are only active when an infected object is active.

Part C – Question 4 …1

4) Explain briefly what potential problem and domain each of the statements or code fragments is associated with, and what a likely effect would be.
   a. Username: ‘; drop table users—
   b. srand(time());
   c. strcpy(wriggle, “Polymorphic”);
   d. while(1) { alert(“This is not a JavaScript alert.”); }

Part C – Question 4 …2

a. Username: ‘; drop table users—

This seems to be a form of SQL injection to bypass the query. The likely effect is that the table users will be deleted from the database.

Part C – Question 4 …3

b. srand(time());

The random number is generated by seeding time. If random password is generated using this method, the adversary can do the same if the adversary knows the rough time when the password is generated.

Part C – Question 4 ...4

c. strcpy(wriggle, “Polymorphic”);

This can cause buffer overflow as strcpy does not perform any bound check. The likely effect is that an adversary may include a malicious code and change the return address to the address of this malicious code.

Part C – Question 4 ...5

d. while(1) { alert(“This is not a JavaScript alert.”); }

This code may cause a non-stop alert pop-up which would irritate the user causing inconvenience such as restarting the computer.

Part C – Question 5 …1

5) Consider the following statements and answer the subsequent questions:

Alice can climb trees and push walls.
Bob can climb trees, push walls and jump walls.
Chris can push Alice, push walls and climb walls.
Dan can climb trees and push walls.

a. What are the subject, objects and actions for this scenario?
b. 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 5 …2

c. If we want to efficiently determine all the actions available to a subject, which of the two list representations are appropriate and why?
d. Assuming the statements were not going to change, could we simplify the representation of access control using some sort of grouping? Explain your answer carefully.

Part C – Question 6 …1

6) The following questions relate to database security.
   a. Name and describe two methods of providing protection against inferential attacks.
   b. What is the purpose of a role in a database system?
   c. Name and describe two of the ACIDity properties.
   d. In what way do the entity integrity and referential integrity rules relate to the consistency of a database system?

Part C – Question 6 …2

a. Name and describe two methods of providing protection against inferential attacks.

   i. Try to design a database in such a way that inferences is reduced.
   ii. Attempt to reject specific/sequence of queries which may lead to inference attack.

Part C – Question 6 …3

b. What is the purpose of a role in a database system?

The purpose is to organize the granting of privileges base on least (minimal) required privileges by job scope or functional activities.

Part C – Question 6 ...4

c. Name and describe two of the ACIDity properties.

ACIDity properties refers to the atomicity, consistency, isolation and durability of database transaction properties. Two ACID properties are **consistency** and **durability**. A consistent database transaction can be thought of as not violating any integrity constraints during its execution. Durability is the property guaranteeing that transactions that have been committed will survive permanently.

Part C – Question 6 …5

d. In what way do the entity integrity and referential integrity rules relate to the consistency of a database system?

Entity integrity is that all the values of the primary attribute must be inserted and referential integrity is that the database must not contain unmatched foreign key values. A database is said to be consistent if the transaction does not violate the entity and referential integrity rule.

Part C – Question 7 …1

7) The following questions cover a range of topics.
   a. Name and describe the two type of error rates that occur in authentication systems, and in intrusion detection systems.
   b. Which of the two rates from the previous questions are more important? Explain.
   c. How does the interpretation of the error rates differ between authentication systems and intrusion detection system? Give an example.
   d. What is the purpose of IDIP?
   e. What does anomaly modelling look for and how do we measure this?

Part C – Question 7 …2

a. Name and describe the two type of error rates that occur in authentication systems, and in intrusion detection systems.

- The two type of error rates that occur in authentication systems are **False Acceptance Rate (FAR)** and **False Rejection Rate (FRR)**. False Acceptance Rate (FAR) is the proportion of authentication or detection attempts resulting in false acceptances. False Rejection Rate (FRR) is the proportion of authentication or detection attempts resulting in false rejections.

Part C – Question 7 …3

b. Which of the two rates from the previous questions are more important? Explain.

It depends. Sometimes we would prefer one over the other while sometimes we want an equal false acceptance and rejection rate which is also known as equal error rates.

Part C – Question 7 ...4

c. How does the interpretation of the error rates differ between authentication systems and intrusion detection system? Give an example.

The interpretation of error rates between authentication system and intrusion detection system has opposite interpretation. In authentication system, FAR is the ratio of the number of false positive divided by the number of identification attempts, while in intrusion detection system, FAR is the ratio of the number of false negative divided by the number of detection attempts.

Part C – Question 7 …4

A false positive in authentication is serious because the authentication system has falsely accepted an intruder, that is, the authentication has identifies a login as acceptable when the login is actually an attack. On the other hand A false negative in intrusion detection system is bad because in this case, the intrusion detection system identifies an activity as acceptable when the activity is actually an attack.

Part C – Question 7 …5

	Intrusion Detection	Authentication
False positive	We are aware of false positive	We are NOT aware of false positive
False negative	We are NOT aware of false negative	We are aware of false negative

Part C – Question 7 …6

d. What is the purpose of IDIP?

IDIP an abbreviation for Intrusion detection and isolation protocol. Its purpose is to stop an attack by blocking the connection between the source of an attack and the target of the attack. It works by detecting an attack and blocking the connection to the target from the source and inform the previous node about the attack which then blocks the connection and inform its previous node until which the connection is blocked from the source to the target.

Part C – Question 7 …7

e. What does anomaly modelling look for and how do we measure this?

The anomaly modelling looks for an outlier, which is an abnormal event that has exceeded the predefined threshold. In an IDS, we have a threshold counter which is twice the sum of the weight of all the event for a day. If the day's anomaly counter goes over the threshold anomaly then the alarm is trigger.

Part C – Question 8 …1

8) Explain what each of the following are, explaining the motivation and/or context for each as part of your answer:
   a. Login Trojan horses
   b. Master passwords
   c. Ping of Death
   d. TOCTOU

Part C – Question 8 …2

a. Login Trojan horses:

   Login Trojan horse is a virus. It has a pop-up so that the user can enter the credential to the illegitimate site thinking that the site is legitimate, but once the credential were entered then it will sent to phisher for his use.

Part C – Question 8 …3

b. Master password:

Is a single password where all the properties are applied to that password instead of many other passwords that are less secured. Typically it is used as the main password used to protect sensitive information such as other passwords and certificates.

Part C – Question 8 ...4

c. Ping of death

Ping of death is a denial of service (DOS) attack. It exploits the vulnerabilities of hosts with weak implementation of TCP/IP stack. When the attacker sends an ICMP Echo request packet with a size larger than 65,535 bytes and that cause the receiver to overflow when the packet is included in the reassemble process. This lead to the target system to crash and a reboot is necessary. It is an attack on availability.

Part C – Question 8 ...5

d. TOCTOU

It is an abbreviation for Time Of Check, Time Of Use. It is an attack that targets a race condition occurring between the time of check (state) for a resource and the time of use of the resource. This attack is possible when two or more concurrent processes are operating on a shared file. For example, the first access is a check to verify some attribute of the file, followed by a call to use the file. An attacker can alter the file between the two accesses.