


National University of Computer and Emerging Sciences, Lahore Campus

	Course Name:	Information Security	Course Code:	CS3002
	Degree Program:	BS (CS)	Semester:	Fall 2022
	Exam Duration:	2 hours 30 mins	Total Marks:	64
	Paper Date:	13/12/22	Weight:	45
	Exam Type:	Final exam	Page(s):	9

Student : Name: _____ Roll No. _____ Section: _____

Instruction: If you think some information is missing then make assumption and write it clearly.

Question 1 a: MCQs and True/False

[10 Marks] [CLO 1]

1.1 _____ virus directly infects the files on the secondary memory.

- a) Resident
- b) Temporary resident
- c) Swapping memory
- d) Non resident

1.2 _____ penetration testing is performed without informing the company's IT department.

- a) Internal
- b) External
- c) Covert
- d) None of the above

1.3 Which of the following properties must a cryptographic hash function provide?

- a) Collision resistance
- b) One-to-one mapping of input to output
- c) Difficulty of finding an input that matches a given hash
- d) All of the above

1.4 The best model to manage conflict of interest is:

- a) BLP
- b) Biba
- c) Clark-Wilson
- d) Chinese wall model

1.5 Demilitarized zone (DMZ) should NOT contain the organization's _____ server.

- a) Web
- b) DNS
- c) Email
- d) Database

1.6 A MAC provides _____

- a) Confidentiality and integrity
- b) Integrity and authentication
- c) Confidentiality and authentication
- d) Confidentiality, Integrity and Authentication

1.7 A trusted third party who provides a way for one party to learn the public key of another party. Web browsers have a list of these trusted third parties, to support communication using HTTPS.

- a) Registration Authority
- b) Certification Authority**
- c) Revocation Authority
- d) None of the above

1.8 A certificate revocation list (CRL) is published as soon as a certificate is revoked.

- a) True
- b) False**

1.9 An attraction of public key cryptography is that, if implemented properly, the algorithms generally run much faster than those for symmetric key cryptography.

- a) True
- b) False**

1.10 Address Space Randomization is a compile time defense against buffer overflow attack.

- a) True
- b) False**

Question 2: [2+2+3+3] [CLO 1]

- a) Explain how longer passwords are more secure than shorter ones!**

If password hashes get leaked, it takes more time to brute-force longer passwords as compared to shorter ones.

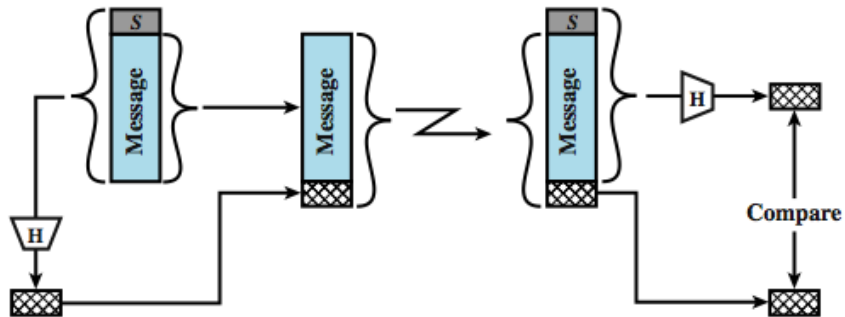
Longer passwords are harder to guess and/or shoulder surf.

- b) Parties A and B carry out a Diffie-Hellman Key Exchange, using a polynomial $p=33$ and generator $g=8$. Party A chooses a private key of 3, while B chooses 2. Show the equation for calculation of their public keys.**

Party A $\rightarrow 8^3 \bmod 33$

Party B $\rightarrow 8^2 \bmod 33$

- c) There are multiple ways to ensure the message authentication and one of them does not require any encryption. Draw a diagram that shows message authentication without using any encryption.



- d) Encrypt the following plaintext using a transposition cipher key 4132.
SENSITIVE MESSAGE

4	1	3	2
S	E	N	S
I	T	I	V
E	M	E	S
S	A	G	E

Ciphertext: ETMA SVSE NIEG SIES

Question 3: [3+4+ 3] [CLO 3]

- a) Principle of complete mediation cannot be applied 100%. Analyze the statement as correct or incorrect, and make your arguments.

If complete mediation is enforced 100%, it will greatly reduce the system performance and poorly impact the user experience because every single access to the system will be guarded with security checks.

- b) Suppose you are writing an anti-virus software. You receive hundreds of samples of a single type of malware, but all samples look different. Identify kind of virus is that, and how can your anti-virus software spot it on running systems.

Because every sample looks different, it would be a polymorphic virus (which uses a different encryption routine on each infection), or metamorphic virus (which changes virus body upon each infection).

Anti-virus can detect it statically by looking for malware-like code (such as decryption routines) or dynamically by its behavior monitoring (malware-like actions such as modifying too many files and copying itself to usb drives etc.).

Anti-virus can NOT use simple techniques like checking file size or file hash, these methods won't catch the malware.

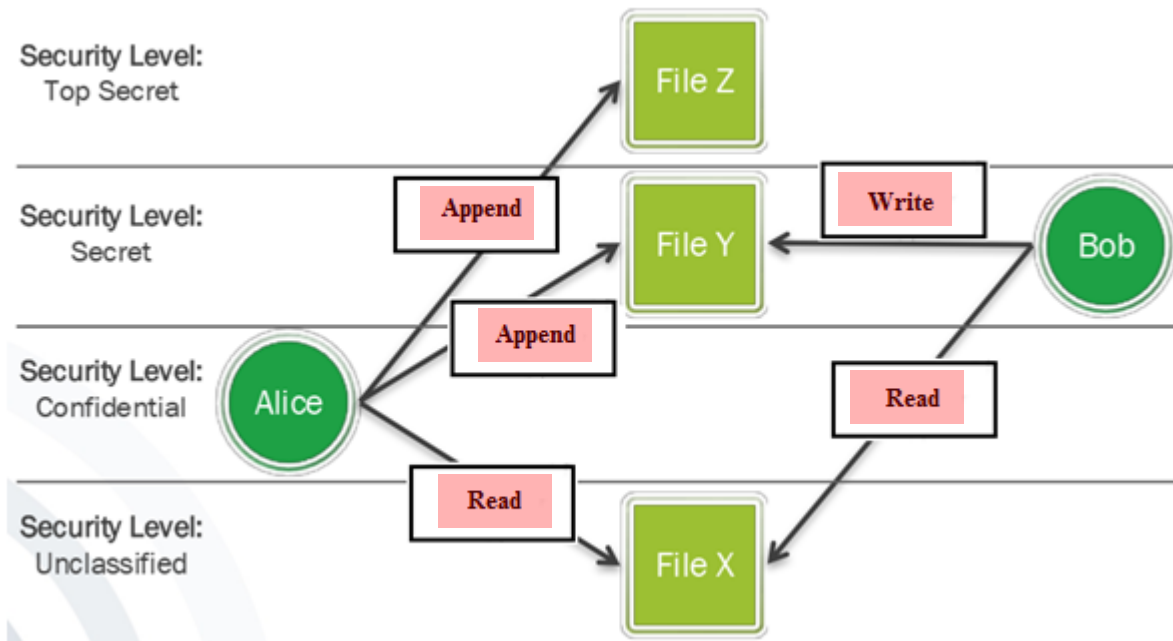
- c) A company wants to securely communicate with their clients using public key cryptography. At the start of communication, both parties exchange their public keys. A client however is concerned that the key they received may belong to an attacker instead. What action should the company take that will make the client believe the received key?

Company should get their public key certified by a CA that is trusted by clients.

Clients can then inspect the certificate and be confident that the key does not belong to an attacker.

Question 4: [5+3+ 2] [CLO 3]

- a) According to Bell-LaPadula Model, which operations can be performed by each subject? Fill each box by the most appropriate operation!



- b) If Bob wants to create something for Alice to be read then at what security level this new object W should be created and do we need any change/addition in security level assigned to subjects.

The new object W needs to be created at Confidential Security level in order to provide read access to Alice. However Bob cannot create it if it is at Secret level. A new role “Confidential” needs to be assigned to Bob in order to create it.

- c) Is it possible to change the security level of an object within BLP model or assign multiple security levels to an object?

No, Within BLP it is not allowed. An administrator could be assigned the responsibility to do it but again such kind of authority is outside the scope of BLP.

Question 5: [3+3] [CLO 4]

- d) Your company produces a ‘medicine reminder’ app for forgetful patients. Firstly, patients record their prescribed medication in the app. Later, the app creates notifications to remind the user whenever it’s time to take the medicine. Upon taking a medicine, patient also records ‘done’ in the app. All data is saved on company servers – app only provides a front end interface.

What are the confidentiality and availability threats for this app? Propose a solution for those threats.

Open ended.

3 marks for (scenario specific) threats, one against confidentiality, second against availability

3 marks for solution of those threats

Question 6: [3+3] [CLO 4]

In overall IT security management, human caused threats are the hardest to deal with due to direct physical access to resources. In your opinion, what could be the possible mitigation strategies in each of the following categories?

a) Employee screening and management

Careful hiring by initial screening and investigation

Employee training

Signing policy agreements

Updating control on termination of employment

b) Technical controls

Restricted access to physical assets

Multi layer authentication

Access Control List

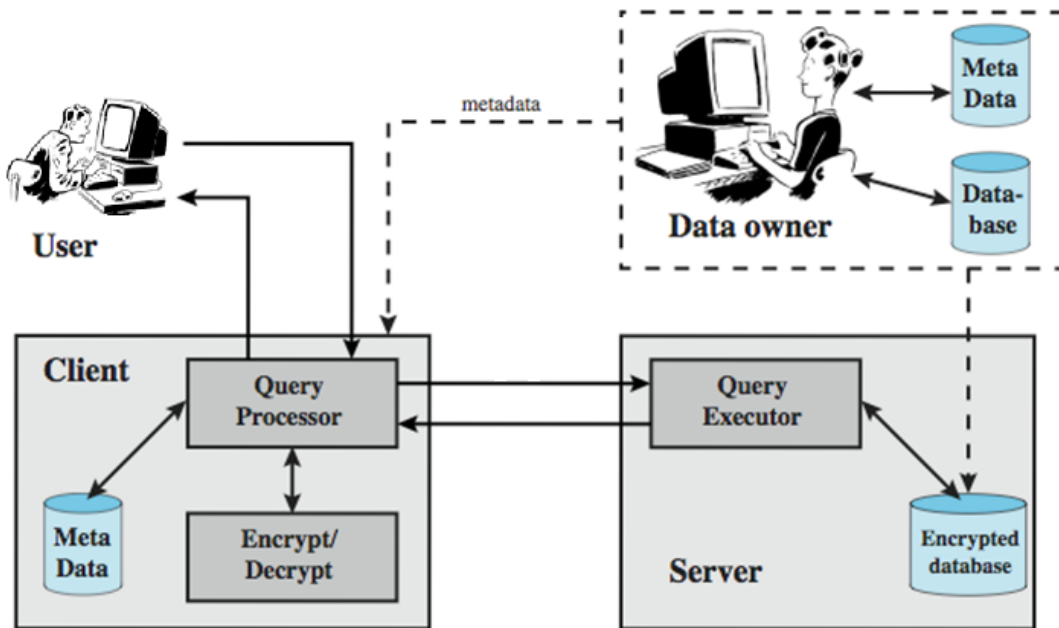
Monitoring through Camera

Keeping logs and records of access

Question 7: [3+4+5] [CLO 3]

Consider the following scenario where we have the following four entities:

- **Data owner:** organization that produces the sensitive data
- **User:** that presents requests (queries) to the system.
- **Client:** Front-end that process the queries
- **Server:** that receives encrypted data from a data owner and makes them available for distribution to clients.



You have to answer the following question:

- a) Which level of encryption (complete DB, Record level or individual fields) will be better to avoid unauthorized access to data of other users without adding unnecessary overhead? Provide reasoning for your selection!

The best option is to do Record level encryption that provides better control on individual records and is less complex as compared to field level encryption. Moreover separate keys can be used for each user if data is for individual users. Even in case of shared data we can make multiple copies encrypted with each user but this will consume extra space!

- b) We can use both symmetric as well as Asymmetric encryption in this scenario. Provide pros and cons of each strategy!

Symmetric Encryption:

All records can be encrypted using either a single private key or creating a separate key for each user. The first option is convenient in terms of management but we can not hide that from different users. The other case is more secure but it will require high cost to manage a large number of private keys and it will keep growing with addition of new users.

Asymmetric Encryption:

In case of Asymmetric encryption Server would have to keep the public keys of all users and it will require specific procedures to do encryption with the public key of intended user who can later access it using its private key.

It provides fool proof security as only the intended user can access its records however in case of share data, multiple copies needs to be stored.

- c) Depict the complete process for the case where Asymmetric encryption has been used. How the data owner produces and saves encrypted records and how each user will access it. You can explain it by a use case considering couple of users and keys involved.

As explained in the last part, Server will encrypt each record with the public key of the intended user and then each one of them can access those records using private key!