FCS Midsem

Vrinda Narayan
2018120

Answer 1.

Part a.

2-Anonymized Table

Identifier	Quasi-Identifier (Insensitive Information)				Sensitive Information	
Customer ID	Name	Place	City	Country	No items purchased	Price
'C00013'	*	*	*	*	'2'	'5000.00'
'C00001'	*	'New York'	'New York'	'USA'	'2'	'3000.00'
'C00020'	*	'New York'	'New York'	'USA'	'3'	'5000.00'
'C00025'	*	*	*	*	'2'	'5000.00'
'C00006'	*	*	*	*	'1'	'10000.00'
'C00002'	*	'New York'	'New York'	'USA'	'3'	'5000.00'
'C00018'	*	'Brisban'	'Brisban'	'Australia'	'2'	'7000.00'
'C00021'	*	'Brisban'	'Brisban'	'Australia'	'1'	'7000.00'
'C00019'	*	'Chennai'	'Chennai'	'India'	'1'	'8000.00'
'C00005'	*	'Mumbai'	'Mumbai'	'India'	'1'	'7000.00'
'C00007'	*	'Chennai'	'Chennai'	'India'	'1'	'7000.00'
'C00022'	*	'Mumbai'	'Mumbai'	'India'	'2'	'7000.00'

Part b.

We used the k-anonymization technique to protect the privacy of the user. Email ID is an identifier and hackers can get access to it through other databases. In such a case, they can correlate their database with the smoking data to determine participants who smoke, putting the privacy of users at risk. To combat this, we need to ensure that the email ID of participants is not available to any adversary, hence we suppress the information using k-anonymization. Any other technique like Randomization, Distributed privacy preservation etc. will not remove the email ID, keeping sensitive information public and not helping in preserving privacy.

Original Data		Anonymized Data	
Email ID	Smoker (Yes/No)	Email ID	Smoker (Yes/No)
iiitd email	Yes	*	Yes
def@gmail.com	Yes	*	Yes
ghi@yahoo.co.in	No	*	No
jkl@iiitd.ac.in	Yes	*	Yes
mno@gmail.com	No	*	No
pqr@gmail.com	No	*	No
stu@gmail.com	No	*	No

Answer 2.

In general there are five major principles

1. Notice/awareness: on how data is being stored and used.
2. Choice/consent: on which data is being collected.
3. Access/participation: to give user freedom to delete or correct data.
4. Security/integrity: to ensure data is protected at all costs.
5. Enforcement/Redress: to ensure the above stated principles are being applied.

However, some regulations have been issued specific to websites with payment gateways as stated below.

1. The responsible party should ensure that no sensitive information of the user like credit card credentials are stored in servers or databases which can be accessed by any adversaries. It is their responsibility to ensure that the confidentiality of user is maintained.
2. No information regarding the user should be stored without their explicit content or knowledge. Information of old users should be deleted and information should be expired after certain regular intervals.
3. In case of refunds, the company should use the same payment method used by the user during the purchase unless stated otherwise by the user.
4. Multi factor authentication should be employed to ensure saved information is not enough for an adversary to complete transactions using a users credentials.
5. The party should employ state of the art security mechanisms and practices, best encryption systems and communication protocols.
6. In case of any security breach in the system, the responsible government authorities should be informed immediately.

7. A regular security report and risk assessment report should be submitted to the responsible authorities to ensure every standard is up to the mark and user data is not at risk.
8. Thorough background checks and competency for all people handling sensitive data should be conducted to ensure that they qualify the requirements and data is not at risk.
9. Security policies of the companies should be reviews periodically by the board to ensure all the standards fit the requirements and are up to the mark.
10. The privacy policy of the company should be clear and easily accessible for everyone to get an idea of what information is being collected and why.

Answer 3.

Assumptions

1. encrypt(m, public_key) can be decrypted only using private_key.
2. decrypt(m, sym_key) can be decrypted only using sym_key.
3. message_from_alice_i is the ith message.
4. unconcat is the unconcatination function and returns [a, b] when input is ab.
5. For part d, we assume private_bob was leaked and is available with Alice as well as the adversary.

Part a.

Bob cannot decrypt the message as he does not have access to private_alice.

Part b.

Bob can decrypt the message.

a. Confidentiality ensured? Yes as only bob has access to private_bob.
b. Non-Repudiation ensured? No as anyone can send the message.
c. Steps to Decrypt
    i. m = unconcat(decrypt(message_from_alice, private_bob))[0]

Part c.

Bob can decrypt the message.

a. Confidentiality ensured? Yes as only bob has access to private_bob.
b. Non-Repudiation ensured? Yes as only Alice can send the signed message (only alice has access to private_alice).
c. Steps to Decrypt
    i. m = decrypt(message_from_alice_1, private_bob)
    ii. Check for non-repudiation
        1. hash_m = hash(m)
        2. hash_m == decrypt(message_from_alice_2, public_alice)

Part d.

Yes, bob can decrypt the message.

a. Confidentiality ensured? No as private_bob was leaked and is available with the adversary.
b. Non-Repudiation ensured? No as anyone can sign the message with private_bob as it was leaked.

c. Steps to Decrypt
    i. m = decrypt(message_from_alice_1, private_bob)

Part e.

Yes, bob can decrypt the message.

a. Confidentiality ensured? Yes, as only bob can decrypt and get access to symmetric key.
b. Non-Repudiation ensured? No, as no signature is sent, anyone can encrypt using public keys.
c. Steps to Decrypt
    i. sym = decrypt(message_from_alice_2, private_bob)
    ii. m = decrypt(message_from_alice_3, sym)

Part f.

Yes, bob can decrypt the message.

a. Confidentiality ensured? No as as Adversary can get access to the sym_1 and sym_2 keys by decrypting using public key of Alice.
b. Non-Repudiation ensured? No. Adversary can decrypt a message, say x1 and x2, using public_alice, take them as sym_1 and sym_2. They can encrypt them using public_bob and send to bob. For the sign, they can simply send x1 and x2 as decrypting them using public_alice would give sym_1 and sym_2, hampering the non-repudiation.
c. Steps to Decrypt
    i. sym_1 = decrypt(message_from_alice_2, private_bob)
    ii. sym_2 = decrypt(message_from_alice_4, private_bob)
    iii. m' = decrypt(message_from_alice_5, sym_1)
    iv. m = decrypt(m, sym_2)

Answer 4.

1. Summary of the System: Multiple students have submitted their assignments to an online platform for evaluation. The Instructor and TA's have access to said submissions for grading. The Instructor or the TA's may have downloaded the submissions into their local devices.
2. Assets
    a. Assignments submitted by the students
    b. Passwords to personal devices of TAs and Intructor
    c. Password to online accounts of TAs and Instructor
    d. Online submission software
    e. Laptops or computers of TAs and Instructors
3. Adversaries
    a. The professor
4. Vulnerabilities
    a. Data stored in local machines is relatively much easier to access.
    b. Weak passwords or problems with cryptography systems.
    c. Gaps and weaknesses in online testing sofware.
5. Threats
    a. Gaining Access to the Machine

i. Try to find a TA or the instructor who is vulnerable to Social Engineering or Phishing. Try to obtain the password of the specific person for their laptop or computer device which they use for grading assignments.
ii. If that fails, try to do keystroke analysis to determine their typing patterns and passwords. Or write a code for brute force analysis on their system utilizing their personal information available publicly.

b. If required files can be found stored locally
   i. Try to gain direct access to the computer to gain access to the documents. However if that is not possible, try remote access attacks like SSHing to the machine or finding vulnerable IP addresses or running a simultaneous access session which is cracked.
   ii. A Trojan can also be sent to the computer of a person via a false submission or email to download all the files present in their system into our own database and gain access to them.

c. If files are not found locally
   i. After gaining access to their machine, we can try to crack the passwords of their online accounts where assignments are stored by trying a Password Resetting Attack on the service which instructors use for assignments.
   ii. SSL Stripping can be performed in the user's connection to make it less secure and easier to crack.
   iii. We can perform a Man in the middle attack to gain access to the connection between the user and the server and get access to the communication in between the two.

d. Trying to attack the server
   i. If the server uses SQL, we can try to perform an SQL Injection to gain access to its database where potential passwords and even assignments of students will be stored.
   ii. We can try to attack the Firewall of the server by IP Spoofing and trying to bypass the firewall to gain access to confidential information.
   iii. A DNS attack can also be performed to reroute the traffic and gain access to user or server packets.

Answer 5.

Part a.

1. Social Engineering: Finding out password with malicious intent using human interaction and psychological manipulation.
2. Brute Force Attack: Using brute force trial and error of different exhaustive options to guess the password.
3. Hash Chain and Rainbow Table Attack: Original password value of hash tables is created using hash chaining brute force.
4. Password Resetting: Manipulating the website to generate a password reset link and creating a different password known by the adversary.
5. Keystroke Logging: Logging the keys typed by the person while filling their password and trying to decipher it accordingly.

Part b.

1. Passwords should not be stored in the server as plaintext. They should be stored as hash tables not accessible to the adversary combating against Rainbow Table attacks. Even if the secret key of the server is leaked, passwords stored should still be secure.
2. The user should have the flexibility to choose and modify passwords as required. However, the same should not be possible for any adversary who might try a password resetting attack.
3. The administrator should not be aware of the passwords and they should not be revealed to anyone. Even if an actual password is known through keystroke logging or social engineering attacks, the scheme should contain additional security measures to combat the same.
4. Incorrect password attempts should be detected by the scheme and login attempts should be flagged. Multiple incorrect logins shouldn't be allowed, combatting against brute force and hash chaining attacks. In such a case, the scheme should ensure adversary cannot access sensitive data.
5. The scheme should not be impractical. It should be user friendly and the passwords should be easy for users to remember. The computations shouldn't take much time, it should be simple and efficient. The scheme should also be scalable in a large setting.

Part c.

1. ASCII Characters from 1 to 127 inclusive
    a. Total characters allowed = 127
    b. Possible number of passwords = 127 + 127**2 + … 127**8 = 68212339274678000 (Let this be N)
    c. Probability of password being guessed = 10,000 * t / N = 0.1
    d. Value of time t = 682123392746.78 seconds
2. 'A' to 'Z' and 'a' to 'z' and '0' and '9'
    a. Total characters allowed = 62
    b. Possible number of passwords = 62 + 62**2 + … 62**8 = 221919451578090 (Let this be N)
    c. Probability of password being guessed = 10,000 * t / N = 0.1
    d. Value of time t = 2219194515.7809 seconds
3. Digits '0' to '9'
    a. Total characters allowed = 10
    b. Possible number of passwords = 10 + 10**2 + … 10**8 = 111111110 (Let this be N)
    c. Probability of password being guessed = 10,000 * t / N = 0.1
    d. Value of time t = 1111.1111 seconds

Part d.

1. Hardware and Authentication software in same system
    a. Spoof the authentication software and use your own program in its place or directly gain control of the biometric system.

2. Hardware and Authentication software in different systems
    a. Spoof the communication channel and perform man in the middle attack. The adversary can intercept the link between the two and pretend to be either of the two and carry out communication.

Answer 6.

Part a.

Access Control List contains the permissions of users for a file in the form of a list. It is an alternate way of writing an Access Control Matrix. An access control list stores each column of the matrix with the value it represents.

1. Example Matrix
    a.

	File 1	File 2
User 1	R, W, O	R
User 2	R	R, W

2. Equivalent List
    a. ACL(File 1) = {(User 1, RWO), (User 2, R)}
    b. ACL(File 2) = {(User 1, R), (User 2, RW)}

They are most widely used for applying security at the individual user level especially for specifying access rights to system objects in Unix based systems like Linux, Ubuntu and Mac OS. They are also used for network traffic filtering and determining which packet goes where.

Advantage

1. It is very easy to tell which all users have access to a specific file as all the details are stored together. Thus it is easy to determine the list of subjects which can access a given object.

Disadvantage

1. If we need to check if a given user has access to a given file (subject), we need to traverse the whole list associated with the subject in the worst case adding an overhead.

Part b.

Here, we are assuming the Bell-Lapadula security model for solving our questions which has two main principles.

1. No read up
2. No write down

i. Paul cannot read or write. This is because he has a higher clearance for group C, but no clearance for group B.

ii. Anna cannot read or write because there is no relationship between the two documents and neither one is greater or same than the other.

iii. Jesse can read but not write as she has a higher clearance level so we follow the no write down approach.

iv. Sammi can read but not write as she has a higher clearance level so we follow the no write down approach.
v. Robin can write bu cannot read as he has a lower clearance level than the file and no read up principle is followed.

Part c.

1. If first relevant entry point is applied, Alice is considered part of only Group 1. The policy states that first relevant entry pertaining to a user is considered. Since Group 1 only has access to Read the file, Alice will be unable to Write to it.
2. If any permission in list policy is applied, Alice is considered part of both Group 1 and 2. This policy states that all entry points pertaining to a user are considered. Since Group 2 has Read and Write access to the file, Alice will be able to Write to it.

Answer 7.

Part a.

We need to generate them on a per host pair basis. Number of unique pairs are (n*(n-1))/2 so number of keys will be (n*(n-1))/2 (assuming symmetric keys).

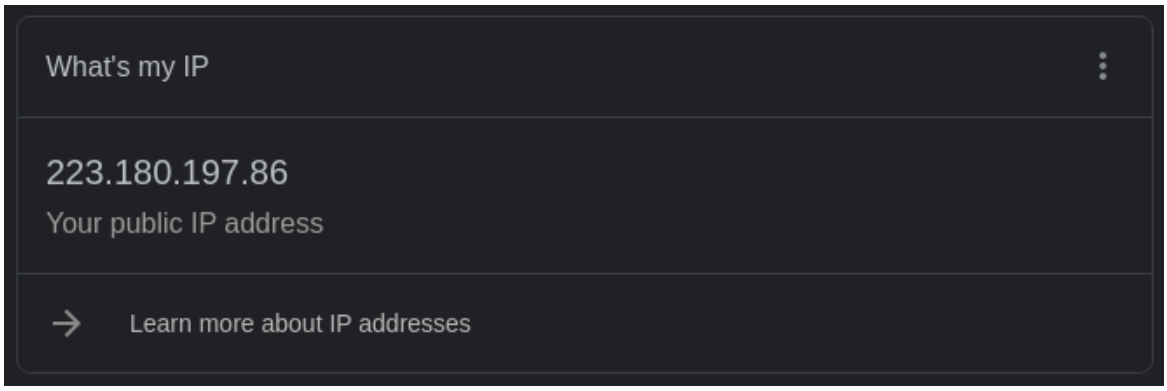
Part b.

The field is present to indicate the next date at which a newer CRL should be available for the system to download.

Part c.

1. A Certification Authority is usually very trustworthy as they are verified and registered. Their reputation and business is at stake so they are very unlikely to be malicious.
2. However, we cannot always trust a CA as they have the power to issue a wrong certificate. If such an issue is caught, all certificates are revoked and the CA is removed from the list of trusted CAs.

Part d.



This IP address is IPV4.

Advantages

1. A lot of existing infrastructure already exists for IPV4 and majority traffic uses it. Hence it has a much greater support as incorporation requieres much lesser effort when compared with IPV6.

2. It is relatively simple and much smaller than IPV6. It is much simpler to put into topological drawings and easier for humans.

Disadvantages

1. Since the range of IPV4 is relatively limited, they are fast becoming exhausted. IPV6 are much higher in number. This increases the cost of using an IPV4 significantly
2. IPV6 have proven to be much faster than IPV4 in terms of internet speeds decreasing the times for site loading.

Answer 8.

I have attended > 95% (11 out of 12) of the classes. I couldn't attend a few in between because my grandma had a major operation and help was needed at home.