FCS MIDSEM

Pandillapelly Harshvardhini
2022345

QUESTION-1 Privacy

PART-A

Here (*) = [0-9]
K=2

Pin Code	Age	Gender	Acc Balance
11002*	30-40	M	150000
11004*	30-40	M	250000
11004*	30-40	M	200000
11002*	30-40	M	250000
11342*	60-70	F	850000
11342*	60-70	F	150000
11342*	50-60	F	850000
11342*	50-60	F	200000
11004*	40-50	M	280000
11004*	40-50	M	450000
11002*	40-50	M	850000
11002*	40-50	M	450000

K=3

Pin Code	Age	Gender	Acc Balance
11002*	30-50	M	150000
11004*	30-50	M	250000
11004*	30-50	M	200000
11002*	30-50	M	250000
11342*	50-70	F	850000
11342*	50-70	F	150000
11342*	50-70	F	850000
11342*	50-70	F	200000
11004*	30-50	M	280000
11004*	30-50	M	450000
11002*	30-50	M	850000
11002*	30-50	M	450000

PART-B

- Pseudonymization

  In this technique there are various methods for data security, like, Data masking which involves hiding the some part of information through the random character like X for example changing the pincode like this “XXXX20”. And also, we can use the random token for each category of the data and that random token is used to access the original data in the future. For example replacing pin code by pincode type “PC001”. By these techniques it will be hard for attackers to crack and identify the information.

- Noise

  In this method we add some random noise in our data like rounding it off, add some meaningful value(Age, weight etc.) to the data or add some random voice to the data. These modifications make it difficult for the attackers to trace back the data. But these values must be chosen carefully if it is too small means it is not sufficiently the data privacy is not that much protected and if its too large then it may lose the data utility.

PART-C

For this particular question these are the GDPR requirements:

- The organization will take a measure in the case of data breach. Under the GDPR rules, the organization will respond to this data breach within 72 hours otherwise the organization will face extra penalties.
- The company privacy and the data processing practices are transparent and allow users to access, alter and view their own data, and data will not be used in ways that are harmful.
- Anonymize the data.
- Pseudonymize the data
- Add Noise to the data
- Clearly specifies why we are collecting data.
- Only collecting the data necessary for the survey purpose. Avoids collecting unuseful or sensitive information.

Now let's choose the techniques and apply it in the dummy data to protect privacy and satisfying the above GDPR requirements also.

DUMMY DATA

Name	Roll No.	Email	Age	Branch	CGPA	Experience
Harshvardhini	22	A@gmail.com	20	CSE	8.0	9
Siri	33	B@gmail.com	20	CSE	7.6	8

Ashok	10	C@gmail.com	22	CSAM	6.4	6
Kirthi	37	D@gmail.com	26	ECE	6.2	10
Anya	07	E@gmail.com	21	CSSS	7.1	7

Applying techniques to protect data privacy.

For anonymity, remove the columns that identify a particular user. For example remove Name, Roll No., Email. And then apply Pseudonymization which replaces these above columns with one column pseudonyms.

To make more private data we can put the data into ranges so that no one guesses the details of the user. For example, make the age in ranges like 20-30.

We can also add some reasonable noise to our data so that it protects privacy.

DATA after applying the above techniques.

S.No	Age	Branch	CGPA	Experience
1	20-30	CSE	8.1	9
2	20-30	CSE	7.8	8
3	20-30	CSAM	6.7	6
4	20-30	ECE	6.6	10
5	20-30	CSSS	7.6	7

- In this I have used Data Anonymization because according to the GDPR personal data should be anonymized if it is going to the third party.
- In the CGPA column I have added the controlled noise by adding its S.No to its corresponding CGPA. This ensures that the one’s response does not impact the results and also prevents attacks.

- Ranges concept is also added in this so that its hard for the attacker to guess the details(Basically k-Anonymity is used).
- Data minimization is also added because according to the GDPR regulations we should only take the data that is relevant to our work.
- Other GDPR principles also are followed and we cannot prove that explicitly. It depends on the website. But in this case as we are using iiitd website so it should follow the remaining principle as it is a trusted website.

So in this way we can prevent the participant's privacy.

PART-D

- Noise addition
  This ensures that small changes do not significantly affect the overall analysis ans also making it harder to guess or predict individual values. And this protects against attribute disclosure attack, in which attacker tries to determine the exact value of a sensitive attribute.
  It may fail in some scenarios like if the noise is too small or could be predicted due to an easy pattern, and the attacker can do reverse engineering to get that data.

- k-Anonymity
  In this it prevents identity disclosure as multiple users share the same group present in the data. And makes it difficult to pinpoint the exact value of an user in the dataset.
  This method may fail because too much information can be lost due to which the data become less useful for analysis and still being vulnerable to re-identification attacks. And if some part of data is grouped into a similar cluster this may reveal extra information to the attacker about the group.

- Data minimization
  This technique ensures that it follows the GDPR’s principle of data minimization, reducing the exposure of personal data.

QUESTION-2 Cyber Attacks

PART-A

In this DNS poisoning attack the attacker change the DNS cache to send the user to the malicious website instead of the original website. In the provided picture in question the attack by attacker can happen in two ways. First, directly getting access to the Alice computer and changing the cache dns stored in the computer. Or attacker 1 will directly change the local DNS server with a large number of requests. We will see the second part.

Steps for attacker 1 to perform DNS poisoning attack:

1. Firstly, Identify the local DNS server connected to Alice by a switch to resolve the domain names.
2. Now attacker 1 has to prepare forged DNS responses which will point to a malicious IP address/website in place of the original one.
3. Now when Alice sends a requests to visit the website, her computer will send a DNS query to LDNS then the attacker 1 analizes this request with the help of tools like Wireshark which analyzes network traffic by capturing packets.
4. Now Before the server replies the Attacker 1 sends the fake DNS response with the malicious IP address. As we know that the DNS servers give priority to the first response so the attacker 1 response will be selected if he send fast then original server response.
5. The fake Ip address is stored in the DNS server. Now the requests from the Alice will take to the malicious site.

This same kind of attack can also be possible when the attacker can access the Alice computer and modify the DNS stored.

PART-B

We can use the following methods for the prevention of ddos attacks:

1. We can identify the normal traffic patterns. By having the basic traffic behaviour of my website it will be easier to identify the anomaly and the unusual behaviour associated with DDoS attack.

2. We should also be able to identify the type of attack. By understanding the type of attack characteristics and applying this to DDos detection program which can detect fast and effectively mitigating the attack before it causes significant damage and making access to the users again.
3. Traffic filtering/ Rate limiting will also be an effective mitigation strategy. In this we can use the Firewall for our web application to filter and block the malicious traffic. This firewall can be implemented on the gateway to effectively blocking attacker 1 and attacker 2. And in rate limiting which restricts the no. of request from single IP.
4. We can also use load balancing which will distribute the traffic to multiple servers. This will prevent multiple requests from the attacker 2.

PART-C

There are various method to set up a secure communication channel for each device:

- TLS/SSL Encryption

  These are the cryptographic protocols that encrypt the data sent between a browser and a server. This prevents attackers from seeing information.

  In this method secure communication begins with TLS handshake. During this the client and server use the public and private keys to exchange the data, during this only the server gives a digital certificate issued by some certificate authority which ensure the client trust. Then using asymmetric encryption during the handshake a secret key (session key) is made which is used to help the communication. Finally, All data is encrypted using a session key and exchanged.

  In the architecture this method can be used between Alice and the Web server. Also between Local DNS and Remote DNS.

- VPN

  VPN creates a secure connection between the device and the remote server. This mask the IP address and hides traffic which protects all the data exchanged between the devices.

  In this first secure tunnel is created then the data is encrypted before being transmitted over the internet which makes sure of privacy. Device authentication happens using the pre-shared keys or certificates. Then Finally Encrypted packets are transferred through

the VPN. This prevents our IP address from reveling in the public and End-to-end encryption.

From the network diagram we can set up VPN between Local DNS server and Remote DNS server. And can use a VPN between Alice and the webserver.

- Key exchange Protocols

  In this Key exchange Protocols like Diffie-Hellman protocols securly shares encryption keys with the help of public and private key.

  First both the parties lets say A and B generate the public and private keys and share the public key over the internet and private keys remain private only corresponding parties can see. Then for example A encrypts the secret key using B's public key and gives it to B then B encrypts using B's private key. Then this shared key is used to encrypt the data for future communication.

  This method can be used during the TLS/SSL handshake for secure key exchange between Alice and the Web server.

- SSH

  We can also use the SSH for secure communication. It is the network protocol that gives users a secure way to access a computer over an unsecured network. It provides authentication and encryption. SSH runs on the TCP/IP protocol.

PART-D

```
Wireless LAN adapter Wi-Fi:

   Connection-specific DNS Suffix  . :
   IPv6 Address. . . . . . . . . . . : 2401:4900:30ee:98c7:fe0f:d5ee:279c:41d2
   Temporary IPv6 Address. . . . . . : 2401:4900:30ee:98c7:a5cf:c708:c46a:132f
   Link-local IPv6 Address . . . . . : fe80::7092:15b3:1ad2:e5d8%14
   IPv4 Address. . . . . . . . . . . : 192.168.184.28
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : fe80::c4bc:b3ff:fe68:8d8f%14
                                       192.168.184.189
```

Advantages of IPv6

- More IP addresses as compared to IPv4
- IPv6 has improved built-in security like Data authentication, Data Encryption etc.

- It has simpler and effective header format compared to IPv4 which increases the speed of the internet.
- Safer compared to IPv4

Disadvantages of IPv6

- Costly, complex and harder to configure
- All the system doesn't supports IPv6

Advantages of IPv4

- Most of the systems and devices are built for IPv4.
- It is simpler and easier to configure
- NAT helps extend the life of IPv4 which will be money saving and prevents us to switching to IPv6
- It is compatible with the most of the networks

Disadvantages

- It has a limited number of IP addresses which was not enough for the growing number of devices on the internet thus in this case we have to switch to IPv6.
- Ip header is more complex which slows down the data processing and routing.
- It does'nt have the built in security features.

QUESTION-3 Building Secure Communication

PART-A

To compromise the HTTPS connection, I would choose the SSL hijacking method and SSL striping method. Because, SSL hijacking allows users to check and decrypt the encrypted data between users and servers by acting like a trusted person. And SSL stripping because it changes the secure HTTPS connection to insecure HTTP connection. This allows the attacker to intercept and steal the information between the victim and the target. These both methods are considered as man in the middle attack.

- To attack through SSL hijacking, first, I execute the man in the middle attack like IP spoofing etc. to catch the victim's connection to the target website. Now without knowing

the user connects to my malicious server, which then i pass the data to its real site. By this I can see or change the users data. If the user tries to use HTTPS, then browsers expect a valid SSL/TLS certificate which I will create a fake certificate to trick the user.

- In SSL striping attack first I try to trick the user computer by poisoning the DNS cache. After tricking the user they connect to my server. Then after this I can change or remove HTTPS redirects.

PART-B

Solution to counter SSL hijacking

The user can prevent SSL hijacking by making sure that he/she cannot be tricked into installing suspicious software that does the fake CA certificate into your system. By avoiding insecure networks like public wifi we can minimize the risk of getting ssl hijacked. We can also use the VPN software.

These measures are effective and highly feasible as they are based on user awareness and cybersecurity practices. And using VPN software which adds extra security of encryption, making it difficult for attackers to attack.

Solution to counter SSL stripping

To prevent this the only way is to use HSTS which guarantees that insecure connections to websites cannot be made. And HSTS forces our browser to upgrade to HTTPS (which is more secure) connection if it is on HTTP connection and also remember that this specific site is accessible through HTTPS only. Now the browser will never attempt to make HTTP to that site again.

Using HSTS is a highly effective solution as it ensures that users cannot accidentally connect to the insecure version of the website. It prevents attackers from downgrading secure connections.

QUESTION-4 Authentication

PART-A

According to picture given in the question this below is happening:

- First, Alice sends a message “I’m Alice” to Bob.
- Now, Bob generates a random challenge(R) and sends this challenge to Alice.
- Then finally, Alice returns R along with the encrypted R using a shared key.

This protocol is basically authenticating Alice by having the proof that Alice has the secret key.

There are few vulnerabilities in this protocols as follows:

- As mentioned in the question that Bob is stateless, this means that he is not able to store the past challenges. This makes it difficult for Bob to detect replay attacks.
- There can be the replay attack vulnerability. Attackers can capture the challenge response pair and they can replay that pair later to show themselves as fake Alice to Bob.
- The protocol doesnot have any mechanism to check whether the parties are actually communicating with each other or it is communicating with the attacker. Attackers can intercept the message “I’m Alice” and make a new session with Bob. Then the attacker receives the challenge “R” and then relays it to Alice and gets the Key that is encrypting R. This allows the attacker to Authenticate as alice later.
- There is no mutual authentication between Bob and Alice.
- No confirmation that the message is coming from real Alice.

So, the protocol is not secure due to reply attacks, and no mutual authentication.

PART-B

Mutual authentication means it ensures that both the parties verify each other's identity before secure communication. If only one of them has a verifiable certificate(lets say Bob has a verifiable certificate issued by trusted CA) still mutual authentication can be achieved using asymmetric cryptography.

Steps to ensure secure communication:

- Bob can authenticate itself to Alice using a certificate and a digital signature. Using Bob's public key Alice can verify and confirm Bob's identity by checking the digital signature(Bob’s private key) from the certificate which should be from a trusted Certificate Authority.
- Now without using the certificate for Alice, Alice can still authenticate itself to bob using the challenge-response mechanism. Bob sends challenge to Alice. Alice encrypts the challenge using the secret key and sends it back to Bob. Then Bob decrypts the data and verifies it from the original challenge. In this way Alice can authenticate itself to the bob.

Cryptographic Information Used in above method

- Private key (of Bob) signature is used on verifiable certificates issued by CA.
- Public key of Bob is used so that Alice can verify Bob's identity.
- Digital signatures: Bob has a verifiable certificate issued by a CA in which a digital signature will be there to prove identity.

This will increase some sought of security but it is still not secure. In this man in the middle attack still can happen when bob sends the challenge to alice in man in the middle can take that challenge. And if CA is not trusted in that case also it will not be a secure protocol.

QUESTION-5 Network Anonymity

PART-A

No, perfect anonymity is not possible on the internet. There are always some ways to track the user. The advanced tools and techniques like Tor, VPSs etc enhances the anonymity. But as said above, absolute anonymity cannot be achieved due to many factors like technical, human vulnerabilities etc.

Here is the reasons,
In systems like Tor, there is an exit node which decrypts the traffic before forwarding it to the website that you want to access to. But if someone is controlling the exit nodes can see the unencrypted data and privacy is not maintained. This controlling exit nodes by someone else is difficult because of the onion routing technology. But the entity who owns the entry and exit nodes has access to the exit node also who can see the information.

If actors like the Government whose statements cannot be denied can give our data to the government for investigation or any other purposes. In this way anonymity is not achieved.

As we know that humans are not machines and they cannot be that accurate. So, by human error also anonymity cannot be achieved. Users can reveal the data without knowing that they are revealing it.

PART-B

Tor basically relies on onion routing to encrypt and through the onion network it reroute the web traffic. Now when user sends a message through tor, first that data is encrypted in layers same

as the layer of the onion. Now the data is transmitted through the series of network nodes called onion routers each of which decrypts(peels away) the layer of encryption to see the next peel of onion. It do like this until the data reaches the final layer. Now the last layer decrypts the last layer of the encryption (now fully decrypted data) and sends the data to its final destination.

It uses the concept of Tor circuit. In which Tor transmits the encrypted packets through these three nodes i.e. entry, middle and exit. In this each node decrypts the layer of encryption, which ensures no single node knows the origin and destination of the data. After a certain time period the new circuit is created which prevents traffic analysis attacks.

Entry Node: This node removes the first encryption layer and passes requests to the next(middle node) in this pass it will ensure that sender's identity is hidden for the upcoming nodes.

Middle Node: This node removes another encryption layer. This node cannot know who is the original sender and also the final sender. And it forwards the request to the next nodes.

End Node: It removes the final layer of encryption and sends the request to the website which the sender wants to visit in.

PART-C

Exit Node Vulnerability

- Since Tor traffic exits through the exit node before reaching to its final destination and we know the exit node decrypts the data and any data that is not encrypted can be read or modified by the operator who operates the exit node which leads to privacy breaches.
- Exploitation
  Running multiple exit nodes to capture the data, And targeting popular websites with HTTP traffic.

Traffic Analysis Attack:

- In this attack attacker tries to analyze patterns which goes from the entry node to exit node to de-anonymize users.

- To exploit this vulnerability we can use statistical analysis to match incoming and outgoing traffic patterns.

Confirmation attack

- In this attack the Tor network allowed the attackers to track the user activity. The attacker can change the traffic passing through the nodes. By looking at these changes the attackers can check whether a user is visiting a particular website or not.
- Using this attack we can monitor the targeted users like journalists, activists, or politicians who are searching for illegal content.

References - Next Page

References

Question-1

- https://www.youtube.com/watch?v=-GBhYvcIRCM&ab_channel=GauravAmeta
- https://www.immuta.com/blog/k-anonymity-everything-you-need-to-know-2021-guide/#:~:text=If%20k%3D2%2C%20the%20data,data%20in%20the%20data%20set.
- https://www.auditboard.com/blog/gdpr-compliance-checklist/?utm_source=chatgpt.com
- https://satoricyber.com/data-masking/data-anonymization-use-cases-and-6-common-techniques/

Question-2

- https://www.okta.com/identity-101/dns-poisoning/#:~:text=DNS%20Poisoning%20(DNS%20Spoofing)%3A%20Definition%2C%20Technique%20%26%20Defense,-Learn%20why%20Top&text=During%20a%20DNS%20poisoning%20attack,like%20passwords%20and%20account%20numbers.
- https://www.indusface.com/blog/best-practices-to-prevent-ddos-attacks/#:~:text=By%20limiting%20the%20amount%20of%20traffic%20that%20can%20be%20sent,to%20avoid%20blocking%20legitimate%20traffic.
- https://www.fortinet.com/resources/cyberglossary/ddos-protection#:~:text=Common%20DDoS%20mitigation%20techniques%20include,)%20for%20application%2Dlayer%20protection.
- https://www.geeksforgeeks.org/differences-between-ipv4-and-ipv6/

Question-3

- https://www.invicti.com/learn/mitm-ssl-hijacking/
- https://www.invicti.com/learn/mitm-ssl-stripping/

Question-4

- https://developerhelp.microchip.com/xwiki/bin/view/applications/security/asymmetric-use-case-example/

Question-5

- https://techofide.com/blogs/vulnerabilities-in-tor-is-the-tor-browser-safe/
- https://www.avast.com/c-tor-dark-web-browser