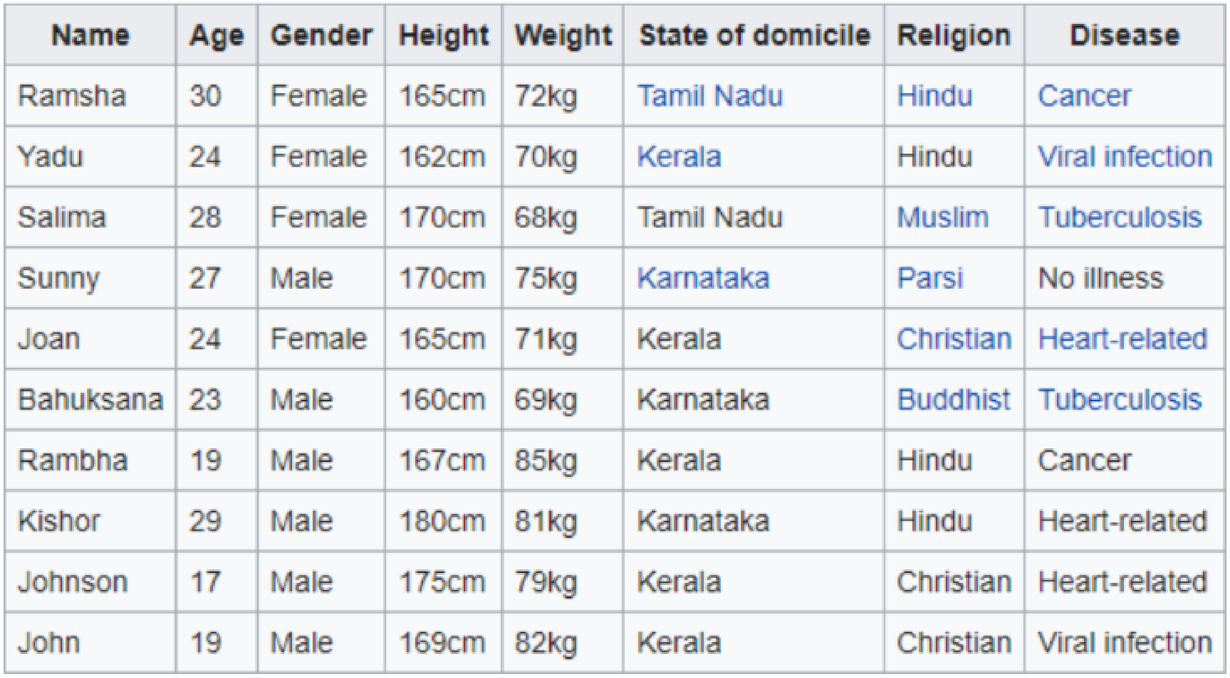
Student name: Chaitanya Arora Student ID: 2021033

CSE 345/545 Foundations to Computer Security

Mid-Sem Exam

1. Privacy [20]

a. Apply K-Anonymity with value of K as 2 and 3. Submit the anonymized tables. [6]



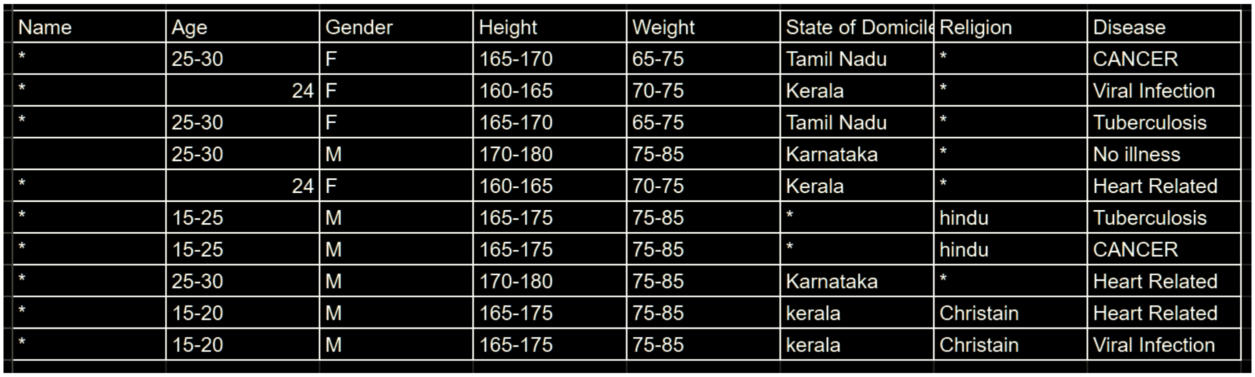
Name	Age	Gender	Height	Weight	State of domicile	Religion	Disease
Ramsha	30	Female	165cm	72kg	Tamil Nadu	Hindu	Cancer
Yadu	24	Female	162cm	70kg	Kerala	Hindu	Viral infection
Salima	28	Female	170cm	68kg	Tamil Nadu	Muslim	Tuberculosis
Sunny	27	Male	170cm	75kg	Karnataka	Parsi	No illness
Joan	24	Female	165cm	71kg	Kerala	Christian	Heart-related
Bahuksana	23	Male	160cm	69kg	Karnataka	Buddhist	Tuberculosis
Rambha	19	Male	167cm	85kg	Kerala	Hindu	Cancer
Kishor	29	Male	180cm	81kg	Karnataka	Hindu	Heart-related
Johnson	17	Male	175cm	79kg	Kerala	Christian	Heart-related
John	19	Male	169cm	82kg	Kerala	Christian	Viral infection

Answer1:

Ans a. Applying 2-anonymity means that any row in the table must be indistinguishable from at least one other row with respect to the sensitive identifiers.

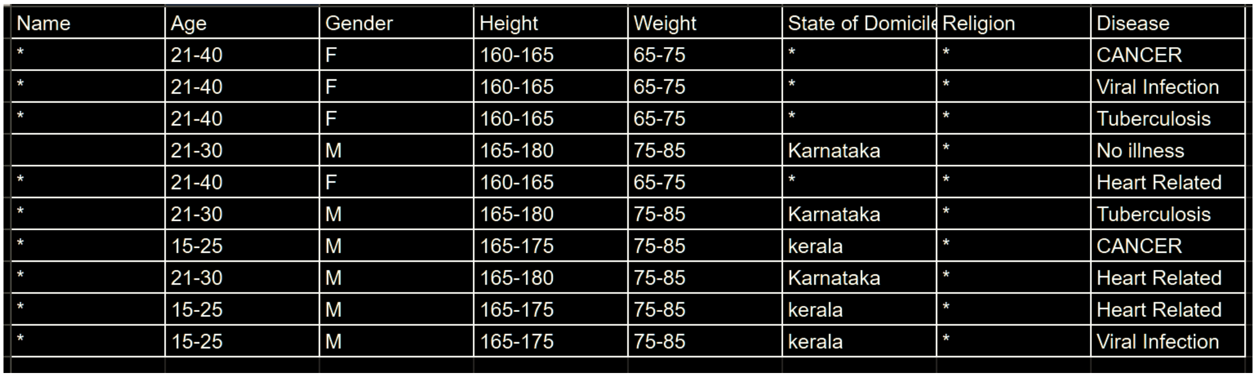
I am making the assumption that gender, state of domicile and religion arent sensitive identifiers and hence I havent applied anonymity there. While sending this data to a 3rd party the sender can choose to omit out these rows as these arent something which can be represented in ranges like other parameters. And I believe that Disease is the main purpose of the dataset and it shouldnt be modified.

After applying 2-anonymity the data will be as follows:



Name	Age	Gender	Height	Weight	State of Domicile	Religion	Disease
*	25-30	F	165-170	65-75	Tamil Nadu	*	CANCER
*	24	F	160-165	70-75	Kerala	*	Viral Infection
*	25-30	F	165-170	65-75	Tamil Nadu	*	Tuberculosis
	25-30	M	170-180	75-85	Karnataka	*	No illness
*	24	F	160-165	70-75	Kerala	*	Heart Related
*	15-25	M	165-175	75-85	*	hindu	Tuberculosis
*	15-25	M	165-175	75-85	*	hindu	CANCER
*	25-30	M	170-180	75-85	Karnataka	*	Heart Related
*	15-20	M	165-175	75-85	kerala	Christain	Heart Related
*	15-20	M	165-175	75-85	kerala	Christain	Viral Infection

After applying 3 anonymity the data will be as follows:



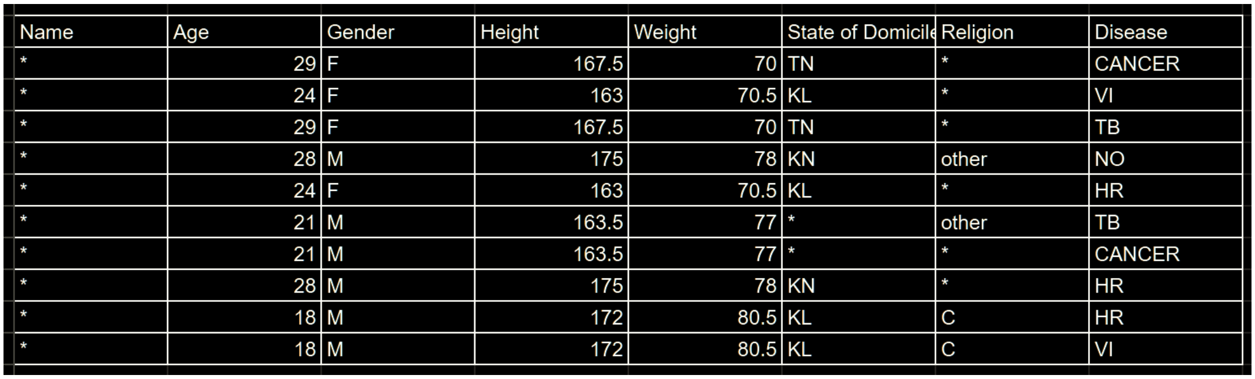
Name	Age	Gender	Height	Weight	State of Domicile	Religion	Disease
*	21-40	F	160-165	65-75	*	*	CANCER
*	21-40	F	160-165	65-75	*	*	Viral Infection
*	21-40	F	160-165	65-75	*	*	Tuberculosis
	21-30	M	165-180	75-85	Karnataka	*	No illness
*	21-40	F	160-165	65-75	*	*	Heart Related
*	21-30	M	165-180	75-85	Karnataka	*	Tuberculosis
*	15-25	M	165-175	75-85	kerala	*	CANCER
*	21-30	M	165-180	75-85	Karnataka	*	Heart Related
*	15-25	M	165-175	75-85	kerala	*	Heart Related
*	15-25	M	165-175	75-85	kerala	*	Viral Infection

b. What techniques (at least two) would you do to increase the utility of the above anonymized data? Demonstrate. [7]

Answer b:

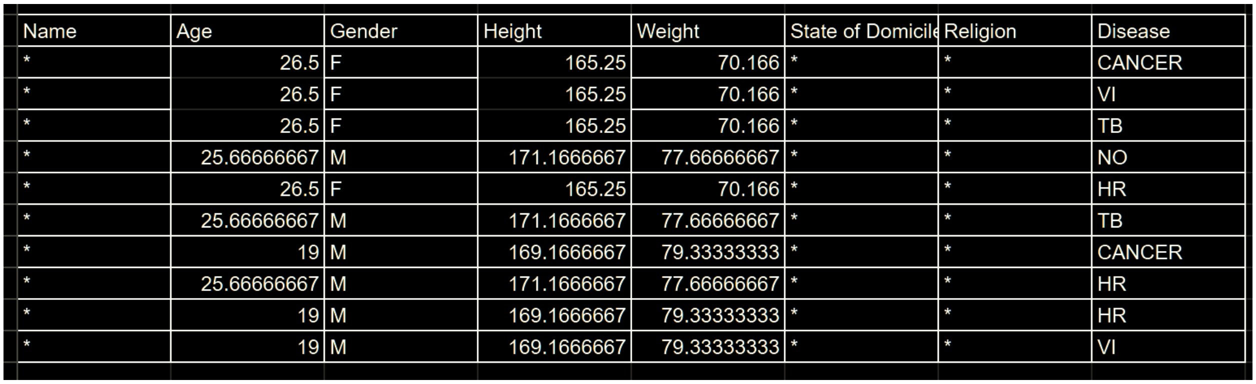
1. If we were to send this data to a 3rd party we would have to omit the columns such as Gender,State of Domicile and Religion as we can do little to put them in ranges so therefore in order to include these columns we can use techniques like: Hierarchical Generalization in which we take the set of Row Values of a particular column and then we go on to divide them into buckets so as to preserve anonymity and make data more mreaningful. In context of the given tables we can use generalization in religion and categorize religions such as Buddhisim and parsi in the category of other religions as its unique to its position in the data.
2. Another thing we can do in the data is to take a window of some size, lets just say K, and then we can club K-rows and replace their values their respective row values by either average or median of the row values that are present in the window. This would increase the utility of the data and protect anonymity.

Following is the table after applying the above two:



Name	Age	Gender	Height	Weight	State of Domicil	Religion	Disease
*	29	F	167.5	70	TN	*	CANCER
*	24	F	163	70.5	KL	*	VI
*	29	F	167.5	70	TN	*	TB
*	28	M	175	78	KN	other	NO
*	24	F	163	70.5	KL	*	HR
*	21	M	163.5	77	*	other	TB
*	21	M	163.5	77	*	*	CANCER
*	28	M	175	78	KN	*	HR
*	18	M	172	80.5	KL	C	HR
*	18	M	172	80.5	KL	C	VI

For 2 window size



Name	Age	Gender	Height	Weight	State of Domicile	Religion	Disease
*	26.5	F	165.25	70.166	*	*	CANCER
*	26.5	F	165.25	70.166	*	*	VI
*	26.5	F	165.25	70.166	*	*	TB
*	25.66666667	M	171.1666667	77.66666667	*	*	NO
*	26.5	F	165.25	70.166	*	*	HR
*	25.66666667	M	171.1666667	77.66666667	*	*	TB
*	19	M	169.1666667	79.33333333	*	*	CANCER
*	25.66666667	M	171.1666667	77.66666667	*	*	HR
*	19	M	169.1666667	79.33333333	*	*	HR
*	19	M	169.1666667	79.33333333	*	*	VI

For 3 window size.

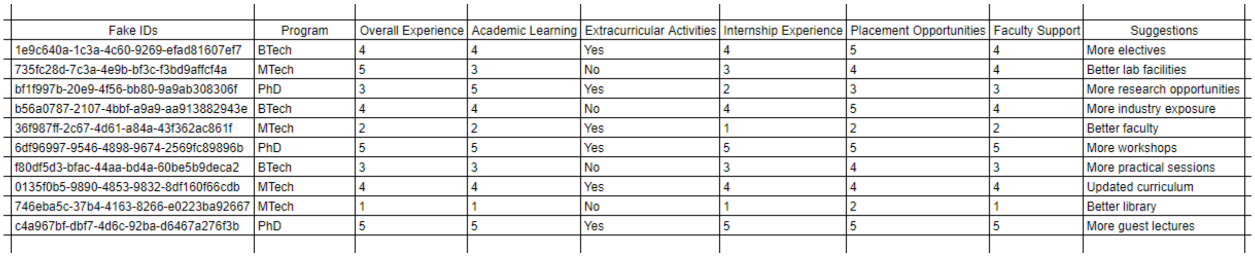
c. Academic department of IIIT-Delhi wants to conduct a survey for outgoing students about their experience. They want to do their best in protecting the privacy of participants' and they need your help. Prepare dummy data of participants. Choose techniques you have learned during the class to protect the participant's privacy in line with GDPR requirements. Explain why you chose it, along with its application on the dummy data you created. [7]

Answer c. GDPR on their website has checklist and they claim that if we follow that checklist then we are in accordance with their standards.

Suppose that in the survey following information was asked:

1. Program in which they were enrolled: like Btech, mtech etc
2. Thier overall experience in a scale of 0-10
3. Their academic Learning in a scale of 0-10
4. Did they participated in extracurricular activities
5. Rating of their internship experience
6. Rating of their research experience
7. Rating of Placement opportunities they received from TnP cell
8. Faculty Support Rating
9. Suggestions for improvement.

Data would be as follow:



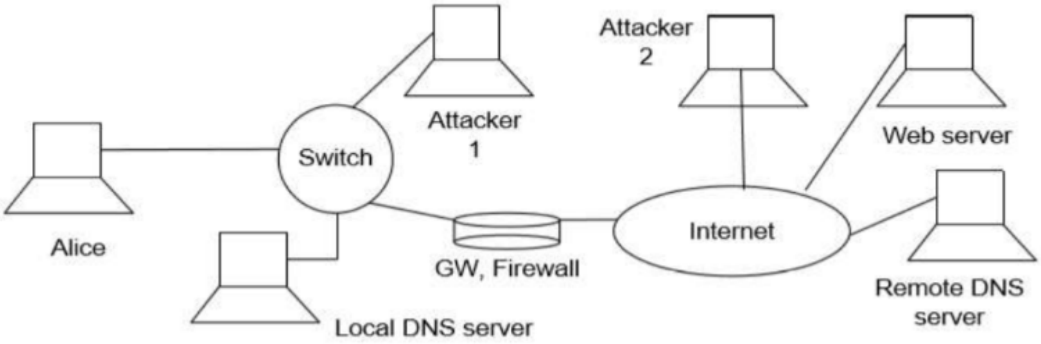
Fake IDs	Program	Overall Experience	Academic Learning	Extracurricular Activities	Internship Experience	Placement Opportunities	Faculty Support	Suggestions
1e9c640a-1c3a-4c60-9269-efad81607ef7	BTech	4	4	Yes	4	5	4	More electives
735fc28d-7c3a-4e9b-bf3c-f3bd9affcf4a	MTech	5	3	No	3	4	4	Better lab facilities
bf1f997b-20e9-4f56-bb80-9a9ab308306f	PhD	3	5	Yes	2	3	3	More research opportunities
b56a0787-2107-4bbf-a9a9-aa913882943e	BTech	4	4	No	4	5	4	More industry exposure
36f987ff-2c67-4d61-a84a-43f362ac861f	MTech	2	2	Yes	1	2	2	Better faculty
6df96997-9546-4898-9674-2569fc89896b	PhD	5	5	Yes	5	5	5	More workshops
f80df5d3-bfac-44aa-bd4a-60be5b9deca2	BTech	3	3	No	3	4	3	More practical sessions
0135f0b5-9890-4853-9832-8df160f66cdb	MTech	4	4	Yes	4	4	4	Updated curriculum
746eba5c-37b4-4163-8266-e0223ba92667	MTech	1	1	No	1	2	1	Better library
c4a967bf-dbf7-4d6c-92ba-d6467a276f3b	PhD	5	5	Yes	5	5	5	More guest lectures

Now as you can see:

1. Instead of using their real names and identifiers we have used fake anonymous ids, which cant lead us to the responders.
2. We should inform to the students why we are collecting the information in order to establish trust and explainability
3. We can store the data in encrypted format
4. We can also give an option for students to request for their responses.
5. We can generate synthetic data for external audits, processings outside the institution like with some third party or orthe organizations
6. We can have an option for students to ask for deletion of data and we can then obey that.
7. Always ensure that we arent compromising on anonymity and storage of data.

Source: https://gdpr.eu/

2. ***Network Security [25+5]***



Answer2.

Describe how attacker 1 to perform DNS poisoning attack. Describe step-by-step procedure. [6]

a) The target is identified and that is Alice in this case.

   Secondly, we will prepare a fake look alike and feel alike website that Alice visits regularly like iiitd.ac.in and then host it on a malicious server to deceive Alice into putting their credentials.

   Then we can use a tool like Ettercap, a network security tool for man-in-the-middle attacks. They configure Ettercap by modifying the “etter.dns” file to include the name of the website they want to attack www.iiitd.ac.in and the IP address of their own server hosting the fake web-page.

   Launch Ettercap in Unified Sniffing Mode: Attacker 1 opens Ettercap in sudo mode and selects Sniff>Unified Sniffing. This allows Attacker 1 to sniff traffic on the LAN network and identify devices connected to Switch, including Alice’s computer and the Local DNS Server.

   From the list of devices displayed in Ettercap, Attacker 1 selects the IP address of Alice's computer (Target 1) and the IP address of the default gateway (Target 2).

Activate DNS Spoof Plugin: Attacker 1 activates the “dns_spoof” plugin in Ettercap. This plugin sends fake DNS responses to Alice's computer, resolving www.iiitd.ac.in to the IP address of the Attacker’s computer where the fake webpage is hosted.

Spoof DNS Response: The attacker bombards Alice's computer with spoofed DNS responses, which makes her computer cache a poisoned DNS record. The Transaction ID in the DNS query and response could be exploited by the attacker making multiple guesses since it’s a 16-bit binary number(this is my assumption)..

Redirect to Phishing Website: When Alice tries to visit iiitd website, her computer refers to the poisoned DNS cache and she is redirected to the attacker’s fake IIITD webpage instead of the legitimate site.

Credential Harvesting: Alice, believing the fake site to be legitimate, enters her credentials. Attacker 1 now has unauthorized access to Alice’s login information and can potentially gain access to sensitive information or systems.

Source: https://ettercap-project.org/

Attackers can DDoS your website. How would you efficiently mitigate the attack and restoreaccess to your site from both the attackers? Defend your solutions [8]

b) We can make use of the following ways to protect ourselves from the DDoS attacks:

We can make a network system akin to that of a CDN system, wherein the traffic is distributed across multiple servers across the world. This reducess the load on the origin server and also mitigated the risk of attack by serving through the nearest server and possiblly making services available to other users.

DDoS Protection Services: Utilize DDoS protection services like Cloudflare, Akamai, or AWS Shield, which have the capability to detect and mitigate large-scale DDoS attacks by redirecting traffic through their networks and filtering out malicious traffic.

Apply rate limiting to restrict the number of requests a user can make in a given timeframe, helping to prevent abuse of your application's API or user login page. Additionally, maintain and regularly update a blacklist of IP addresses known to be malicious.

When elevated traffic levels target a host, a fundamental protective measure is rate limiting, which ensures the host only accepts traffic within its handling capacity to maintain availability. Advanced protection techniques further scrutinize the legitimacy of the traffic by analyzing individual packets. This necessitates an understanding of the typical characteristics of legitimate traffic received by the target, enabling a comparative analysis against this baseline for each incoming packet.

Source:

https://www.namecheap.com/blog/how-a-cdn-can-help-protect-against-ddos-attacks/

How would you set up a secure communication channel for each device in the above architecture?[Bonus if you can set it up without involving third-party service and offline key exchange?] [5+5].

c) There are a number of procedures we can follow to ensure that the communication channel setup between the devices on the given architecture can securely communicate.

In the given scenario, Alice can use the Diffie-Hellman algorithm to establish shared keys with the local DNS server, the web server, and any other entities she communicates with. This allows them to establish secure communication channels without prior contact, offline key exchange, or third-party services.

While Diffie-Hellman algorithm provides a way to establish a shared secret, it does not authenticate the parties involved.

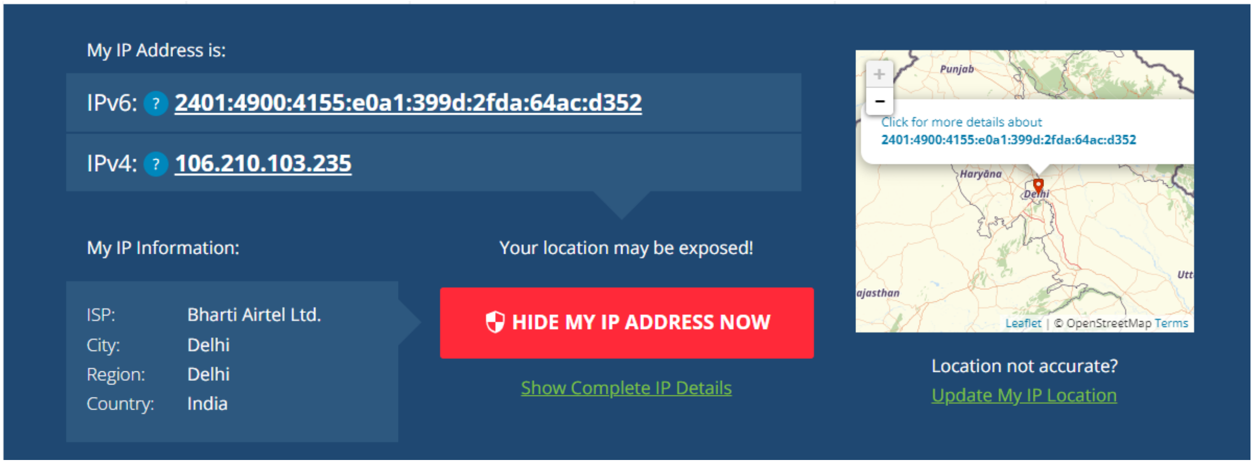
We can also configure the gateway firewall to only allow necessary traffic between VLANs and the internet, blocking any unauthorized access or communication.

The local DNS server, when communicating with the remote DNS server, should utilize DNSSEC (Domain Name System Security Extensions) to validate DNS responses. DNSSEC is designed to protect against DNS spoofing by digitally signing DNS data. It ensures that the DNS responses received by the local DNS server have not been altered in transit and originate from a legitimate source.

To ensure secure communication with the web server, Alice should utilize HTTPS, which integrates Transport Layer Security (TLS) to safeguard the confidentiality and integrity of exchanged data. It is vital for Alice's client to validate the server's SSL certificate, confirming communication with the legitimate server and mitigating the risk of Man-in-the-Middle (MitM) attacks.

Turn on your phone's hotspot and connect your laptop to the network. Check your IP address. Is it Ipv4 or Ipv6? Share a screenshot of the IP address as well. Also, state the advantages and disadvantages of the type of IP address you get. [1+2+3]

D)



My IP Address is:

IPv6: 2401:4900:4155:e0a1:399d:2fda:64ac:d352

IPv4: 106.210.103.235

My IP Information:

ISP: Bharti Airtel Ltd.
City: Delhi
Region: Delhi
Country: India

Your location may be exposed!

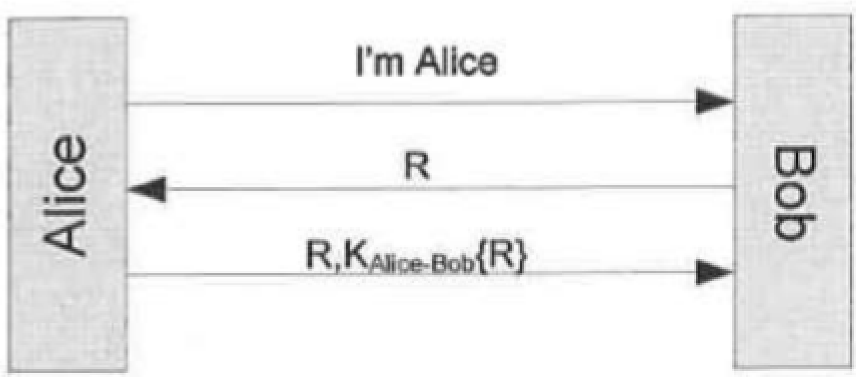
Utilizing both IPv4 and IPv6 addresses simultaneously is referred to as the Dual Stack method. This approach facilitates a seamless transition and ensures compatibility as the internet evolves.

Advantages: IPv4 has been a foundational technology, with extensive use across internet traffic, guaranteeing compatibility due to its ubiquitous support. Its maturity and optimization, derived from extensive utilization, make it a robust protocol. Furthermore, the comparatively concise nature of IPv4 addresses enhances their readability and user-friendliness

Disadvantages: The protocol's address space is restricted to approximately 4.3 billion unique addresses, a quantity rapidly nearing exhaustion. The antiquity of IPv4 means it lacks inherent security mechanisms capable of thwarting contemporary threats without the integration of additional protocols such as IPsec. The depletion of unique public IPv4 addresses necessitates the implementation of Network Address Translation (NAT), which imposes additional configuration requirements

Advantages: IPv6 offers a significantly expanded address space, eliminating the issues of address depletion and enabling direct addressing. This expansion negates the requirement for NAT, fostering end-to-end connectivity and enhancing the functionality of peer-to-peer networks and services such as Voice over Internet Protocol (VoIP). Furthermore, IPv6 optimizes routing efficiency by reducing routing table sizes and incorporating inherent security mechanisms like IPsec.

Disadvantages: The complexity of IPv6 addresses can be daunting for users. The lack of universal support for IPv6, coupled with the absence of inherent communication capability between IPv4 and IPv6 hosts, necessitates the adoption of practices like dual stacking and tunneling to maintain connectivity during the transitional phase. The transition to IPv6 represents a significant investment, with many enterprises perceiving minimal short-term returns. Additionally, the novelty of IPv6 means that literature on the protocol is limited, leading to a practical scenario where security experts may find IPv4 more familiar and, consequently, potentially more secure due to established practices.



Answer 3:

(a) Suppose we are using a three-message mutual authentication protocol and Alice initiates contact with Bob. Suppose we wish Bob to be a stateless server, and therefore it is inconvenient to require him to remember the challenge he sent to Alice. Alice sends the challenge back to Bob, along with the encrypted challenge. Is the protocol (presented below) secure? Justify your answer. [4]

a) No, this protocol is not secure. This protocol is susceptible to the replay attack. If an attacker capture the message contaning R from Bob to alice, they could potentially reuse teh message in a later session to impersonate Bob, since Bob is a stateless machine and doest not remember sending R, it might accept the replayed R as valid when sent by attacker.

Also it has a potential MITM vulnerability. The attacker could capture the message send by Bob initially and change the value R to R2 then receive the message from Alice and so on and so forth.

Therefore without additional mechanisms in check this method could lead to safety of messages getting compromised.

(b) Is a common key necessary for setting up secure communication channel? How can both parties' safely setup a common key? What are its limitations? [6]

b) Yes, indeed a common key is necessary to set up a secure communication channel because otherwise the confidentiality of the data will be compromised, and sending the data as plain text would mean that any person who can capture the packets exchanged between the two people and intercept the raw messages. Safely setting up a key can be done through various methods, one such popular method of exchanging keys is deffie-hellman which allows two parties to setup a common key over an insecure communication channel. Another such method could be using an asymmetric key, where one party encrypts a generated secret key with other party's public key before sending any communication. And in this method the encrypted data can only be decrypted using private key of the other party.

Limitations of the Deffie-hellman key exchange:

1. MITM: Man-in-the-middle attacks are possible in this scenario in which you could be setting up a secure symmetric key with the attacker who is sitting in the middle of the both parties.

Limitations of Public key Private Key:

1. The overall complexity of using this type of mechanism is a lot when it comes to exchanging large amounts of information using this methodology.

Some common limitation are as follows:

1. If keys are compromised, the communication cannot be secure.
2. Another such flaw is that if lets just say that someone has kept a track of all the packets over the communication channel and he has kept a record of all the exchanges between Alice and Bob, suppose at a later point when the communication was over the key got compromised then all the packets that were encrypted or decrypted using that key can be decrypted and hence these types of mechanisms arent past proof, if a key is compromised then all previous communications are considered to be compromised.

(c) How can the above limitations be overcome to set up secure communication channel, is it possible for attacker(s) to launch successful MITM or spoofing attacks? Justify [6].

c) The above limitation can be overcome in the following ways:

1. To reduce the complexity of the public key private key cryptography we can use this mechanism to set up a secure symmetric key and then proceed with using symmetric key for communication. This will eliminate the MITM attack.
2. To make sure that a key compromise doesnt lead to much damage we can employ the use of temporal keys, like some keys that expire after some time or are time dependant so that they can be used to decrypt the data after certain amount of time or better still some mechanism in which the keys keep on shifting or rotating after successsive usage in some secretive manner so that determining what key was used in which exchange would be a difficult task.

It would be difficult to MITMs to intercept messages which are set using mutual authentication. We can make use of CA Certification Authorities to verify the authenticity of the public keys and can help ensure that parties communicate with the intended entities, thus reducing the risk of these types of attacks.MITM attacks or spoofing attacks are possible in which the keys are established by the exchange of information on the communication channel about setting of the keys.

(d) Can you perform mutual authentication if only one party has verifiable certificate, if yes what cryptographic information do we use set up secure comm? Is it secure? Why? [4]

d) Absolutely mutual authentication can indeed be achieved even when only one party holds a verifiable certificate. This scene is commonplace in client-server architectures; the server presents a certificate verified by a trusted Certification Authority (CA), while the client does not share this privilege. The client checks the server's identity using the server's certificate, and on the flip side, the server may employ alternate mechanisms to authenticate the client, such as employing a username and password or a client-spawned key.

In a setting where one party possesses a verifiable certificate, the use of asymmetric cryptography emerges as a viable pathway to concoct a secure communication channel. The certified party can unveil its public key to the other party in a secure manner, given the authenticity of the public key can be verified through the certificate. Subsequently, the other party can generate a symmetric session key, encrypt it with the certified party's public key, and send it back securely. Upon receipt, the certified party can decrypt it with its private key, both parties now share a common secret key for symmetric encryption, which is renowned for its speed and efficiency in ongoing communication.(Also describe the same in answer to the last part)

This arrangement can promise security, provided the cryptographic algorithms employed are robust and the implementation is devoid of flaws. The use of a verifiable certificate from a trusted CA acts as a cornerstone in establishing trust in the identity of one of the parties, thereby reducing the risk of man-in-the-middle MITM and spoofing assaults.

The security of this setup is linked to the trustworthiness of the CA, the potency of the cryptographic algorithms employed, and the security mechanism of the private keys.

If the way of checking the identity of the party without a certificate is not strong, or if there are mistakes in the cryptographic methods or how they are put into practice, the safety of the communication can be at risk.

In the initial protocol described, where Bob is a stateless server and the authentication is based on sending back a value received from Bob along with a made-up key, the lack of a strong authentication process and the lack of a certificate for Alice makes the mutual authentication and the setup of secure communication doubtful.

4. Access Control [10]

Consider the following scenario. Alice owns file Z. Alice has read and write access to file X and write access to file Y. Bob owns file X. Bob has read access to file Y and read, write, and execute access to file Z. Carol owns file Y. Carol has read access to files X, Y, and Z.

a. Given a system with many transient users and several persistent protected resources, which technique, ACL or Capabilities, is more efficient for storing and managing users' permissions? Give justifications for your answer. [2]

Answer 4.

a) We have multiple transient users and several persistent protected resources. Although both ACL and Capabilities can perform the functions required, Capabilities would be more efficient for storing and managing user's permissions. In ACL, we have a list of users for each file, while Capabilities is more user oriented. Since we have multiple transient users, in ACL we would have to make changes on each file for a single user. Thus, by using capabilities, we would have to make lesser changes and is hence more effective.

ACL: Permissions are stored with resources, growing the ACL size with more transient users, increasing storage needs. Scalability issues with many transient users and resources, leading to slower permissions checks and complex management.

Capabilities: Permissions are stored with users, discarded as users leave, potentially better for storage efficiency. Scales better as permissions are user-centric, managed independently of resources.

b. In ACL/Capability is it possible for an unauthorized user/process to misuse privileges of Alice to write/read contents of file X? How? [4]

b) In the ACL access control lits, unauthorized access could occur through impersonation. A plausible scenario of this is seen in a Trojan Horse. Carol, owning file Y, writes a trojan horse program onto file Y. Bob, with read access to file Y, then executes the trojan horse, which then accesses file Z, which is owned by Alice, and writes its contents onto File X, which Alice has write permissions to. In this intricate way Carol tries to indirectly write to File X, by bypassing the access controls and misusing Alice's privileges.

In capabilities systems, unauthorized access could manifest through capability leaking or delegation, mainly if capabilities are not securely managed. In a hypothetical scenario, if Alice unknowingly delegates her capabilities to Bob, and Bob has malicious intent or his capabilities are further leaked to Carol, who harbors malicious intent, the cycle of misuse could ensue, leading to unauthorized access and potential data tampering on File X.

Although both the approaches have their flaws I would stil have chosen Capabilieties based approach as the management would have been easier and so would threat mitigation.

c. How can you prevent such unauthorized access? Elaborate your response. [4]

c) One approach to achieving this is through the bell-la-padula model. By applying clearances to subjects (users) and labels to files, strict access control is established, ensuring that users interact with files in a manner conforming to predefined security policies.

The bell-la-padula model works under three rules

First, the "No Read Up, No Write Down" (NRU, NWD) principle.

Under the "No Read Up" (NRU) rule, users are only permitted to read objects at their own security level or below, preventing the leakage of sensitive information to lower clearance levels. The "No Write Down" (NWD) rule restricts subjects to writing to objects at their own security level or above, eliminating the potential spillage of higher-level information to lower-level domains. Derived from the combination of NRU and NWD is the "No Read Write Up Down" (NRWUD) rule, which restricts subjects to reading and writing operations solely on objects at their own security level.

However BLP model also has some limitations which can be solved using a combination of both BLP and RBAC security systems. This role-centric model is particularly effective in dynamic environments where transient users are prevalent. When roles are assigned to users, they automatically inherit the necessary clearance levels to interact with resources securely as per BLP's guidelines

Source: https://ieeexplore.ieee.org/document/4806931

5. Network Anonymity [15+5]

a. Is perfect anonymity possible on Internet? Provide justification for either of your answers. [4]

Answer 5.

a. Assuming that human error and lapses in judgment remain constants, the pursuit of achieving absolute anonymity on the internet is a distant dream. Protocols integral to the internet's function, such as TCP/IP, necessitate the exchange of identifiable information, thereby inherently compromising user anonymity. Furthermore, web browsers send unique device specifications, leaving a distinctive fingerprint that can be exploited for tracking, effectively circumventing traditional privacy safeguards. Moreover, even anonymizing tools, which are highly valuable, such as Tor, are not im,mune to vulnerabilities and potential compromises, thereby leaving user identities susceptible.

   Nonetheless, if a group of people were to momentarily suspend the consideration of human fallibility and naivety, and hypothetically invest considerable resources in the creation of a synthetic persona—imbibed with all the attributes and behaviors characteristic of a real individual—there emerges a plausible argument for the attainability of anonymity. In such a scenario, a group of people might maintain anonymity to the extent that their authentic identity remains concealed, revealing only the fabricated persona they are amenable to leave and completely disassociate from. This methodology implies operating on a nuanced level that precedes even the backstage, interacting with the digital realm through a meticulously constructed façade, thereby rendering the quest for true identity an intricate endeavor.

   Pardon me for becoming a little philosophical in my previous response and I also discussed the same with Prof Arun Balaji Buduru during lectures and we agreed to disagree.

b. How does tools such as TOR build secure anonymous communication channel with acceptable QoS? Explain. [6]

Layered Encryption: Data transmitted through Tor is encapsulated in multiple layers of encryption, like an onion.

Circuit Building: A random path through several nodes in the Tor network is chosen by the system. Each node peels away one layer of encryption to reveal the next nodes address, hence the term Onion Routing\.

Entry, Middle, and Exit Nodes: The chosen path comprises an entry node, middle nodes, and an exit node. The entry node knows the user’s IP but not the final destination, and the exit node knows the destination but not the user’s IP.

Quality of Service (QoS): To maintain an acceptable level of QoS, Tor employs congestion control, traffic prioritization, and various other optimizations. However, due to the inherent design involving multiple hops and encryption/decryption processes, some latency and reduction in speed are to be expected compared to regular internet browsing.

c. Can anonymity in TOR be compromised? Justify. How would you exploit vulnerabilities (at least 2)? [Bonus if you provide zero-day exploits] [5+5]

Indeed, Tor’s anonymity can be compromised, and this vulnerability stems from several inherent weaknesses and potential attack vectors within the system.

One of the key vulnerabilities is the Traffic Analysis Attack. By monitoring the data entering and exiting the Tor network, an adversary has the ability to correlate the timing and volume of the traffic. This means if an attacker can observe the traffic coming into the entry node and going out of the exit node, they could potentially use statistical analysis to match the two and thus de-anonymize users.

Implementing a Traffic Correlation Attack. An attacker, possibly utilizing advanced hacking skills, could gain control or observe both the entry and exit nodes in a Tor circuit. This would enable them to employ statistical analysis to correlate the timing and size of the packets, thereby revealing the user’s identity and the destination.

Additionally, an attacker could exploit vulnerabilities by Compromising Relay Nodes. By setting up malicious Tor nodes, compromising existing ones, and ensuring that users select these compromised nodes, the attacker could analyze traffic patterns and potentially de-anonymize the user.

Sorry, but I tried my best and got so far in the quest of finding some zero-day exploits perhaps all my efforts went into vain, whence I realized that all the potential vulnerabilities and exploits that I had thought had already been thought through by other people. I am only a little late.