Computer Security (COM-301)

Privacy

True or False

(A) A service provider offering easy default privacy preferences for users does not guarantee that the users' privacy is protected from the service provider.

(B) In order to provide anonymity against a state adversary it is necessary that the first and last nodes in a Tor path are owned by different people in different countries.

True or False

(A) A service provider offering easy default privacy preferences for users does not guarantee that the users' privacy is protected from the service provider.

A) True. The privacy preferences are towards other users. What can those see or not see. The service provider sees everything

(B) In order to provide anonymity against a state adversary it is necessary that the first and last nodes in a Tor path are owned by different people in different countries.

B) True. As long as the entry or the exit know is not owned by the state adversary, the state adversary cannot do correlation.

Who’s the fan?

On the music streaming platform OurSpace users can like songs and decide whether their likes should be public (visible by all users), restricted (visible only to their friends on the platform), or private (visible only to the user itself). To be able to stream music on OurSpace, users are required to register with a valid email address.

One of the COM-301 TAs is a big fan of Taylor Swift and wants to like one of Taylor's songs so that more of her music is recommended to him by the platform. Because the TA is very privacy-aware, they are connecting to OurSpace using the Tor browser and only allows his friends to see his likes.

Does this setup provide good privacy to the TA if his main privacy concern is that

(1) The other TAs learn that the shy TA is a big fan of Taylor Swift?

Justify each response. For each of the concerns, explain which of the privacy mechanisms used in this setup protects the shy TA's privacy with respect to this concern. If the shy TA is not protected, explain why not.

Who’s the fan?

On the music streaming platform OurSpace users can like songs and decide whether their likes should be public (visible by all users), restricted (visible only to their friends on the platform), or private (visible only to the user itself). To be able to stream music on OurSpace, users are required to register with a valid email address.

One of the COM-301 TAs is a big fan of Taylor Swift and wants to like one of Taylor's songs so that more of her music is recommended to him by the platform. Because the TA is very privacy-aware, they are connecting to OurSpace using the Tor browser and only allows his friends to see his likes.

Does this setup provide good privacy to the TA if his main privacy concern is that

(1) The other TAs learn that the shy TA is a big fan of Taylor Swift?

Depends on whether the TAs are friends of the shy TA in OurSpace or not

Justify each response. For each of the concerns, explain which of the privacy mechanisms used in this setup protects the shy TA's privacy with respect to this concern. If the shy TA is not protected, explain why not.

Who’s the fan?

On the music streaming platform OurSpace users can like songs and decide whether their likes should be public (visible by all users), restricted (visible only to their friends on the platform), or private (visible only to the user itself). To be able to stream music on OurSpace, users are required to register with a valid email address.

One of the COM-301 TAs is a big fan of Taylor Swift and wants to like one of Taylor's songs so that more of her music is recommended to him by the platform. Because the TA is very privacy-aware, they are connecting to OurSpace using the Tor browser and only allows his friends to see his likes.

Does this setup provide good privacy to the TA if his main privacy concern is that

(2) OurSpace learns that the TA is a big fan of Taylor Swift?

Justify each response. For each of the concerns, explain which of the privacy mechanisms used in this setup protects the shy TA's privacy with respect to this concern. If the shy TA is not protected, explain why not.

Who’s the fan?

On the music streaming platform OurSpace users can like songs and decide whether their likes should be public (visible by all users), restricted (visible only to their friends on the platform), or private (visible only to the user itself). To be able to stream music on OurSpace, users are required to register with a valid email address.

One of the COM-301 TAs is a big fan of Taylor Swift and wants to like one of Taylor's songs so that more of her music is recommended to him by the platform. Because the TA is very privacy-aware, they are connecting to OurSpace using the Tor browser and only allows his friends to see his likes.

Does this setup provide good privacy to the TA if his main privacy concern is that

(2) OurSpace learns that the TA is a big fan of Taylor Swift?

OurSpace sees all likes. Because users can register can link all likes. Thus, no matter the configuration, OurSpace will learn the shy TA is a big fan when they like many Taylor songs!

Justify each response. For each of the concerns, explain which of the privacy mechanisms used in this setup protects the shy TA's privacy with respect to this concern. If the shy TA is not protected, explain why not.

Who’s the fan?

On the music streaming platform OurSpace users can like songs and decide whether their likes should be public (visible by all users), restricted (visible only to their friends on the platform), or private (visible only to the user itself). To be able to stream music on OurSpace, users are required to register with a valid email address.

One of the COM-301 TAs is a big fan of Taylor Swift and wants to like one of Taylor's songs so that more of her music is recommended to him by the platform. Because the TA is very privacy-aware, they are connecting to OurSpace using the Tor browser and only allows his friends to see his likes.

Does this setup provide good privacy to the TA if his main privacy concern is that

(3) The TA's Internet Service Provider learns that he is a big fan of Taylor Swift?

Justify each response. For each of the concerns, explain which of the privacy mechanisms used in this setup protects the shy TA's privacy with respect to this concern. If the shy TA is not protected, explain why not.

Who’s the fan?

On the music streaming platform OurSpace users can like songs and decide whether their likes should be public (visible by all users), restricted (visible only to their friends on the platform), or private (visible only to the user itself). To be able to stream music on OurSpace, users are required to register with a valid email address.

One of the COM-301 TAs is a big fan of Taylor Swift and wants to like one of Taylor's songs so that more of her music is recommended to him by the platform. Because the TA is very privacy-aware, they are connecting to OurSpace using the Tor browser and only allows his friends to see his likes.

Does this setup provide good privacy to the TA if his main privacy concern is that

(3) The TA's Internet Service Provider learns that he is a big fan of Taylor Swift?

Because the TA is using Tor, the communication is encrypted. Therefore the TA cannot see the content and even if they could infer the destination they would not be able to know who they like.

Justify each response. For each of the concerns, explain which of the privacy mechanisms used in this setup protects the shy TA's privacy with respect to this concern. If the shy TA is not protected, explain why not.

Tor vs TLS

Agree or disagree with the following statements:

1) " If a user's connection to a server is protected by TLS, using Tor does not increase the user's privacy towards a local adversary that can only observe the LAN of the client".

2) "If you log into Facebook via Tor, there is no need to use TLS to protect the password from an adversary that can see the connection from your gateway to the entry node and has the capability to perform BGP hijacking on traffic towards Facebook”

Login with Tor

Agree or disagree with the following statements:

1) "If a user's connection to a server is protected by TLS, using Tor does not increase the user's privacy towards a local adversary that can only observe the LAN of the client".

Compared to TLS, Tor hides the server's IP and Server Name Indication (SNI)
Also Tor would hide DNS (requests also go to Tor) while without Tor you need a second protocol (DoH or DoT)

2) "If you log into Facebook via Tor, there is no need to use TLS to protect the password from an adversary that can see the connection from your gateway to the entry node and has the capability to perform BGP hijacking on traffic towards Facebook"

TLS is required as the adversary can do BGP to hijack Facebook's IP to observe the connection.
Without TLS the communication from the exit node to the destination is not encrypted.