Unit 10 - Week 08: P2P Anonymous Communication, The Anonymous Communication on the Internet through TOR Network, An Introduction to TOR Browser, Hidden Services on TOR Network, and Summary of the Course

Assignment_8

The due date for submitting this assignment has passed.
As per our records you have not submitted this assignment.

Due on 2020-11-11, 23:59 IST.

1) Consider the following statements about various kinds of the anonymity and anonymous communication. (It is assumed that Alice is a sender and Bob is a receiver). *1 point*

i. Anonymity protects the identity of a participant in a networked application.
ii. Sender anonymity protects the identity of the sender. Alice sends the message to Bob, and Bob cannot trace Alice's identity.
iii. TOR is a primary tool for maintaining anonymity online.
iv. Receiver anonymity protects the identity of the receiver. Alice can contact Bob, without knowing his identity. Broadcasting achieves receiver anonymity
v. Mutual anonymity guarantees that both parties of a communication remain anonymous to each other as well as to all others in the network.
vi. Anonymous communication systems are often slow.
vii. In bi-directional Anonymity, Alice and Bob communicate without knowing each other's identities.

Which of the above statement/s is/are **NOT** true? Select the correct code.

- i, ii
- iii, v, vii
- iv, vi
- None of the above

No, the answer is incorrect.
Score: 0
Accepted Answers:
None of the above

2) Consider the following statements about the onion routing and TOR network. *1 point*

i. The term onion routing refers to the layered encryption of a message by keys of nodes with their immediate or next hops nodes along the message forwarding path.
ii. TOR is a circuit based low-latency anonymous communication service.
iii. TOR uses AES 128 bit encryption in counter mode for onion routing in order to improve the performance.
iv. A TOR client chooses only three TOR nodes as the message forwarding path which called a TOR circuit or simply circuit. The first node is called entry, the second is middle and the last is exit. The entry knows the sender and the exit knows the receiver. If attackers control the entry and exit, they may correlate the traffic at the entry and exit nodes to find the communication relationship.
v. In anonymous communication, cryptography is not a perfect solution as it protects only the content but not traffic information.

Which of the above statement/s is/are **NOT** true? Select the correct code.

- i, iii
- ii, v
- iv
- None of the above

No, the answer is incorrect.
Score: 0
Accepted Answers:
i, iii

3) There are two statements marked as Assertion (A) and Reason (R). Read the statements. *1 point*

Assertion (A): The Dark Web refers to content that can only be accessed via "darknet," without disclosing the identity of content provider and seeker. It is mostly hidden from Web users and requires specific software.

Reason (R): Dark Web can be created via TOR using multiple encryption layers for the content in transit.

Mark your answer as per the codes provided below:

- A is true, but R is false.
- Both A and R are true, and R is the correct explanation of A.
- A is false, but R is true.
- Both A and R are true, but R is not the correct explanation of A.
- Both A and R are false.

No, the answer is incorrect.
Score: 0
Accepted Answers:
Both A and R are true, but R is not the correct explanation of A.

4) In an Onion Network, Alice (sender) wants to setup a telescopic encrypted tunnel to exit node E. Consider the following sequence of the steps in the network. *1 point*

S1: Alice chooses a path to an exit node E via intermediate Onion Router (OR) node OR1.
S2: Alice send a control cell with command create, circuit id c1 and Random String x1 encrypted by public key part of onion key of OR1.
S3: OR1 decrypts the x1, generates another random string y1, and computes a symmetric ephemeral encryption key k1 using x1 and y1.
S4: OR1 sends a control cell to Alice with command 'extended', circuit id c1, y1 and hash of k1.
S5: Alice receives y1 and computes the symmetric ephemeral key k1 and verified hash of k1 with received hash.
S6: Alice sends a relay cell to OR1 with circuit ID c1, command relay and encrypted payload. The encrypted payload consist of relay command extend, exit node E's IP address, random string x2 encrypted with the public key part of onion key of node E.
S7: OR1 decrypts payload, reads the relay header. Based on command 'relay extend' analyses the data. Send a control cell to E with another circuit ID not used in between OR1 and E, command 'create', encrypted x2 as received in payload.
S8: E decrypts x2, generates another random number y2, computes symmetric key k2, sends control cell with command 'created' with only y2.
S9: OR1 form a message with relay command 'extended', y2, hash(k2), encrypt it with k1 and sends it to Alice with circuit id c1 in relay message.

Which of the above step/s is/are **NOT** correct? Select the correct code.

- S1, S6
- S2, S5
- S3, S7, S9
- S4, S8

No, the answer is incorrect.
Score: 0
Accepted Answers:
S4, S8

5) Consider the following statements. *1 point*

i. The encryption protects the content and identity both.
ii. In modern-day surveillance, in a communication context, metadata is more important and valuable. The metadata is who you talk to, when you talk to, where you talk to, for how long you talk to, how often you talk to, on what device and the software you talk to.
iii. Being anonymous is the same as being private.
iv. Being the complete anonymous on the web, leaving no trace about your presence, is not possible today.
v. TOR is an overlay network that runs on the Internet; the goal of this network is to make it is impossible to trace traffic back to its origin. This is achieved by encrypting and rerouting your traffic at least three independent TOR relays. These relays are run by volunteers around the world.
vi. TOR browser is the easiest tool to get access to the TOR network.

Which of the above statement/s is/are **NOT** true? Select the correct code.

- i, iii
- ii, vi
- iv, v
- None of the above

No, the answer is incorrect.
Score: 0
Accepted Answers:
i, iii

6) Which of the following statement/s is/are **NOT** true for cells in TOR? *1 point*

- In TOR, cells are a communication unit composed of a payload and a header.
- The 512 bytes cells ensure efficient multiplexing of multiple circuits as well as streams.
- Every Onion Router uses a symmetric key to unwrap the cell.
- The Onion Router knows Onion Proxy's IP address via the control cell but does not know the user ID and node ID.

No, the answer is incorrect.
Score: 0
Accepted Answers:
The Onion Router knows Onion Proxy's IP address via the control cell but does not know the user ID and node ID.

7) Consider the following statements about the hidden services? *1 point*

i. TOR hidden service allows users to publish their service without revealing their identity, i.e. IP address.
ii. Users can connect to this service by sending the information about rendezvous point to an introduction point without knowing the publisher of the service and revealing their identities.
iii. The publisher should be able to hide its identity for a long time, and service should bind with only one onion router, the publisher should allow migrating service to different onion routers.
iv. The publisher needs to way to filter incoming request so the attacker cannot flood the service by making many connections to service.

Which of the above statement/s is/are **NOT** true? Select the correct code.

- i
- ii
- iii
- iv

No, the answer is incorrect.
Score: 0
Accepted Answers:
iii

8) Suppose Bob wants to publish a hidden service. Consider the following statements. *0 points*

i. Bob first need to deploy the service on the server. Then he will select few contact points for the service; these contact points are known as the introduction point.
ii. Bob's TOR client generates the public key for each introduction point and these are published along with the service public key in a DHT index or in directory server after signing with the private key for the service. The search key for this record can be derived from service's onion address. Bob makes a TOR circuit (telescopically encrypted) with all introduction point and wait for connections requests to arrive.
iii. This descriptor can be found by the client by requesting xyz.onion where xyz is 16-character name derived from public key of the service.

Which of the above statement/s is/are **NOT** true? Select the correct code.

- i, ii
- iii
- iv
- None of the above

No, the answer is incorrect.
Score: 0
Accepted Answers:
None of the above

9) Suppose Alice has learned about Bob's service, and she wants to access the service. She already knows the descriptor of Bob's service. Consider the following statements. *1 point*

i. Alice wants to communicate anonymously. Her TOR client creates a TOR circuit to a randomly picked relay and asks it to act as a rendezvous point, also send a rendezvous cookie to it for accepting the connection from server.
ii. Alice sends the rendezvous cookie, rendezvous server address to the introduction point, encrypted by the public key of the server corresponding to it. This communication takes place via the TOR circuit from Alice to introduction point and TOR circuit created from server to the introduction point.
iii. The hidden service gets the request and obtains the address of the rendezvous point, and send the one-time secret, second half of DH handshake (y1), to it in a rendezvous message via TOR circuit.
iv. At this point, it is very important that hidden service sticks to the same set of entry guard when creating a new circuit. The entry guard is a set of relays that are always picked as the first node while creating a circuit. These entry guard are chosen randomly
v. In the last step, the rendezvous point notifies the client about the successful connection establishment after matching of rendezvous key. It also passes y1 and hash of symmetric key to Alice. Thereafter both client and hidden service can use their circuits to the rendezvous point for communicating with each other. The rendezvous point simply relays (end-to-end encrypted) messages from client to service and vice versa.
vi. In general, there are six relays used in end to end communication. Three of them are chosen by service, and the other three including rendezvous point, are chosen by the client.

Which of the above statement/s is/are **NOT** true? Select the correct code which shows all correct combination.

- i, ii
- iii, v
- iv, vi
- ii, iii

No, the answer is incorrect.
Score: 0
Accepted Answers:
ii, iii

10) Match Set I with the sentences in Set II: *1 point*

Set I.

A. Surface Net
B. Darknet
C. DeepNet

Set II.

1. It is the collection of all websites that are indexed by search engines.
2. It is the collection of all websites that are not indexed by search engines.
3. It is an important part of the Internet ecosystem. It allows for the publication of websites and the dissemination of information by revealing the publisher's identity or location
4. It is unconventional marketplaces that offer a disturbing range of products or services. You can buy or broker illegal drugs, weapons, counterfeit goods, stolen credit cards or breached data, digital currencies, malware, national identity cards.
5. On this network, contents are hidden intentionally.
6. It is used to anonymously share information with media outlets.
7. It is available to the public.
8. On this network, to find pages is to receive a link to the page from someone who already knows about the page.

- A(1,3,7), B(2,4,5), C(6,8)
- A(1,3), B(2,4,5), C(6,8)
- A(1), B(2,3,4,6), C(5,8)
- A(1), B(2,3,6),C(4,5,8)

No, the answer is incorrect.
Score: 0
Accepted Answers:
A(1,3,7), B(2,4,5), C(6,8)