Home Assignment 2

A-2 Why is it important to have a large volume of traffic in anonymous communication?

You can only be anonymous when there is a large set of users. So, the more people using a certain system, the more anonymity will be possible. It is therefore important to have a large volume of traffic in order to make sure that communication is anonymous.

A-5 What is the purpose of the random value R_0 in a Mix?

The purpose of the random value R_0 is to add some randomness to a message. This is done to avoid the possible usage of guessing attacks.

A-12 Regarding replay attacks on Mixes, two protections are suggested in the lecture notes. Which? Would you say that any of them is the better choice? Show how the two strategies can be combined and how this can make the protection more efficient.

The two suggested protections are *timestamps* and *saving fingerprints*. Both methods are good against replay attacks, but they can both be bypassed. If timestamps are being used, and the attacker is quick enough, the attack might succeed. With fingerprints, or session IDs, the hash of the previous message is saved and compared with the next message. But if the two messages are identical (e.g. if the user wants to withdraw the same amount of money) the message might be thrown away. In the end, timestamps are in my opinion the better alternative since it is more flexible. The best way is to use a combination of the two methods. Then, the messages can be identical but have different timestamps which is fine. A replay attack would then be near to impossible to perform.

A-13 It is straightforward to generalize the N − 1 attack to an N − k attack, 0 < k < N. Describe the N − k attack.

If the attacker controls many messages that are input to a mix, it will be possible to get a good understanding of where they are being sent. In a worst case scenario, the attacker controls all the message going into a mix except one. He or she can then track the target address of that one message (N - 1 attack), making it possible to link sender and receiver. An N - k attack is basically the same, but now the attacker looks for several targets and not one.

A-14 Consider the long term intersection attack. Explain how the number of users and the size of each batch will affect the efficiency of the attack.

It is more difficult to observe messages entering and leaving the mix if there are many users or if the batches are very large. Having many users will increase anonymity making it difficult to perform the attack. It will overall be more difficult to track and store senders.

A-18 Why is onion routing called onion routing?

The name onion routing comes from the fact that messages are encapsulated in layers of encryption, which is analogous to the layers of an onion.

A-23 Several users can use the same exit node in Tor, but different intermediate nodes. How can the exit node know where to send the response from the target?

When the exit node sends the fully decrypted message to the web server it receives it again as a response. It then uses an address table in order to send the response (now again encrypted) back to the previous node which does the same until the message finally reach back to the user.

A-25 Explain what the point of the recognized field in a Tor cell is and how it makes communication more efficient.

The recognized field is there to simply indicate if the cell is encrypted or not. When the cell is being sent, the recognized field is set to zero. When being received and decrypted, if the value is non-zero, the cell has not reached its final destination. Only when the field is decrypted to a zero we can know for sure that the cell has been delivered correctly. This makes for an easy way to check the status of a cell, making communication more efficient.