Anonymous Communication with The Onion Routing Services

Mustafa Saraç

A. Introduction to The Onion Routing Services

In today's world, because of the reason that there is a possible risk on the security and privacy while using the Internet, some of the people, who are concerned about this unwelcome situation, would like to reduce this risk by getting benefit from some technological ways such as onion routing services. The onion routing is a service that provides an opportunity to stay anonymously on the Internet. In this strategy, the messages that will be transferred during the communication are covered in the layers which use encryption to improve the security. In addition, there are nodes, in other saying the onion routers, in this network that map out a route from message sender to the receiver through the communication. However, because of the reason that each of these nodes merely has the information of which node did this message come from and which node this message will be transmitted, this strategy keeps the sender anonymous and the message will be transferred to the destination after the exit node decrypts it. In other words, there is not a direct connection among these communicators; rather, the onion routing services the message is transmitted through the encrypted layers which extends the path. Therefore, some of the people prefer to use the onion routing services in order to become anonymous on the Internet. These people might be the criminal ones or activists that want to hide themselves against the state or even might be the innocent ones that would like to protect themselves against the possible attacks. The purpose of this paper is to discuss TOR, which is one the most popular onion routing services, with its successful and failure points against the possible attacks.

B. How TOR Provide Security and Privacy Against the Possible Attacks

As it is mentioned before the onion routing services provide anonymous communication for the people who are concerned about their security and privacy. One of these services, TOR protects against some of the possible risks and attacks. For example, one possible attack might be done by using the way of traffic anaylsis. This strategy allows to spot the people in their conversations. According to the article that the TOR Project organization explains the details of the project, it is possible to monitor what a person does on the Internet in case of having information about the source and target of this traffic (The TOR Project, Inc). The organization added that the traffic analysis might cause a risky situation if the adversary has an idea about the victim's physical address (the TOR Project, Inc). Traffic analysis pays attention to the header files, which is one member of Internet data packets, in order to get knowledge about the source and target. Thus, some security and privacy mechanisms, such as encryption, does not provide privacy against the traffic analysis because encryption just works for the content of the communication, so it will be possible to still get information from headers due to their unencrypted status. The article stated that TOR minimizes the possible risks of traffic analysis strategy because it works by giving some convenient nodes from the server to the user's client and dividing this users's actions on different locations on the Internet, which provides an indirect random path from source to the target and it is not possible to have an idea about the whole route from an individual node, so this feature gives user the opportunity of staying anonymously on the Internet (The TOR Project, Inc). By this way, TOR prevents the eavesdroppers to get an information on source and target. In addition to these, the organization added that the main point of TOR's security comes from its user diversity, so in the case of

having more TOR users will make it more secure (The TOR Project, Inc). Therefore, TOR improves the security and privacy of its users.

C. In Which Type Of Attacks Does TOR Fail

Even though TOR provides security and privacy against some possible attacks, such as using the traffic analysis, in some cases it might fail due to the person related mistakes. In the article that the TOR Project organization gives advices that are related with staying anonymously while using TOR, it is stated that it is not a good practice to use real personal information on the websites because TOR does not help on possible end-to-end timing attacks, so the adversary might have a chance to get information (the TOR Project, Inc). According to the article that was published by Adam Billman, it is stated that there had been an attack by the National Security Agency (NSA) in 2013 (Wonder How To, 2013). The purpose of this attack is to weaken the anonymity of the users that is provided by TOR. According to the Adam, the main idea of how this NSA's attack works against the TOR comes from the statistical analysis and he demonstrates a possible attack by using the Bayes Theorem (Wonder How To, 2013). He stated that an adversary with a botnet might use latency attack to check the latency on different nodes in the network and might find the message sender by observing this latency after finishing the whole route (Wonder How To, 2013). In addition to these, Adam gave some advices on how to increase the security and privacy. He stated that using a proxy with TOR will improve the protection against the possible attacks and always updating the computer is the essential part of the security in his opinions (Wonder How To, 2013). Edward Snowden, who is the old NSA employee, leaked the NSA documents, which are consisted of some confidential data, in 2013 and after this situation it is seen that even though using some security services, such as the TOR, does not guarantee the security and privacy of the people according to this leaked data.

D. Conclusion

In conclusion, Internet users who care about the online privacy and security tend to use services that help to hide their identities. Going online anonymously can be preferred for different reasons. For example, criminals hide their identity in order to process illegal operations. On the other hand, ordinary people can also go online anonymously to be protected from possible attacks. However, possible attacks still continue even if when a superior service is used, such as the TOR, because of the person related mistakes. Attacks will be possible as long as the users are inattentive.

E. References

The TOR Project, Inc

<https://www.torproject.org/about/overview.html.en>.

Wonder How To 2013, *Use Traffic Analysis to Defeat TOR*

<https://null-byte.wonderhowto.com/how-to/use-traffic-analysis-defeat-tor-0149100/>.