Anonymity and Data Security Related Security Concerns in TOR Network

D.G.G.R JAYASINGHE

Reg. No.:MS20907334

M.Sc. in IT

Specialized in Cyber Security

Supervisor: Mr. Kavinga Yapa Abeywardena

November 2021

Department of Information System Engineering

Faculty of Computing

Sri Lanka Institute of Information Technology

Table Content

Table of Figure

1. ABSTRACT

Working title: Anonymity and Data Security Related Security Concerns in TOR Network

For those unfamiliar with Tor, it is a privacy-enhancing system that is meant to protect Internet users' confidentiality against non-global opponent traffic analysis attempts. TOR is a network protocol that has been developed to provide the anonymous transfer of communication data packets for the transport of low-latency information. Tor is well-suited for mobile devices, such as those used for online browsing, document management, and video conferencing since it provides anonymity on top of TCP while maintaining a rapid reaction time and throughput. Because the communications exchanged over the TOR network are encrypted and the sender stays anonymous, many people believe that the TOR network is safe. TOR, like every other software, contains flaws, which are difficult to detect. Even when TOR is utilized appropriately, there are a plethora of cautions to be aware of. Due to the use of risky protocols in Tor, a malicious router might potentially collect passwords by monitoring exit traffic. While exit routers are monitoring data in such cases, it is quite straightforward to identify the source of the problem. Exit routers are used to capture POP3 traffic in order to breach accounts. Tor is exposed when a router is configured with the default escape policy because it discloses information about the numerous harmful actions that are tunneled via it. Attempts to hack, charges of copyright infringement, and bot network control networks, to name a few examples of malicious communication that may be identified using Tor are all common. There are several types of attacks that may be launched against TOR. Some assaults are designed to cause damage to the Tor client, such as denial of service attacks. Some of them are as follows: The customer is threatened by plug-in assaults, which are carried out via the Web browser that he or she uses to access the network. Certain attacks make advantage of remote technology that has been inserted into the program (a "plug-in"). These applications operate as independent software and are executed on the operating system with the privileges granted to the users by the operating system. ii) The Torben attack manipulates web pages in order to encourage the user to examine information from untrusted sources in order to find a Tor client on their computer. iii) P2P Significant Parameters This kind of attack takes use of Tor clients' connections to peer-to-peer networks in order to deanonymize their communications. TCP/IP packets are sent to a torrent tracker, which is a network service with which a client must contact in order to get information about the list of peers that are able to share the desired resource. Attackers may manipulate the content of the list by inserting a malicious torrent peer's IP address in it, which will cause the list to be re-generated. A suite of assaults known as Raptor, which may be conducted by the Autonomous System in order to deanonymize clients, is described in detail in Section 4. In one attack, traffic analysis of asymmetric communications that characterize the network is used to determine the vulnerability. The suspect's purpose in this form of threat

is to put the secret service in a position of vulnerability by threatening to reveal its identify or undermine it. As previously stated, the Tor network may be used to access apps on both the public surface Internet and Tor (hidden services), as well as applications on the private surface Internet. Some assaults are designed to cause damage to the Tor network's servers. In other cases, the secret service is obliged to connect to a malicious target site during these assaults. Cell counting and padding are two examples of such tactics: During the introduction step of the secret services, the attacker delivers a Tor cell/packet that he has particularly crafted. In order to enter the (malicious) meeting location, the message is transmitted to the secret service, which is requested to construct a Tor chain in order to do so. In addition, Coronate is a program that automatically detects location leaks in hidden services, which is a kind of phishing. Information about a hidden service's IP address may be revealed if sensitive data in the material is disclosed. Most of the time, the administrator is the source of these breaches. Off-path MitM- This kind of attack involves a man-in-the-middle (MitM) assault on a Tor covert operation in order to get access to the Tor network. The fact that the attacker does not have to be in the communication channel is a significant point to consider. To connect and recover data from the Tor network, traffic must eventually depart the anonymized and encrypted Tor protocol, which must be accessed via the "normal Internet" in order for users to link and retrieve data from it. This is accomplished via the use of exit nodes, which serve as virtual gateways through which encrypted Tor communication may be sent to the Internet.

As a result, the proposed study is primarily concerned with the security of information that is sent from the exit node to the server and provides a solution for data security at the exit nodes. The solution is mostly focused on the server side.

2. ACKNOWLEDGEMENT

It gives me great pleasure to express my gratitude to everyone who contributed to the realization of this thesis. To my parents, who have always been there for me and prayed for me, thank you. My Boyfriend is the one to whom I owe my deepest gratitude and affection. Their support and assistance have been invaluable to me during my MSc., and they have done so in a number of ways. I am eternally grateful to them for all of their aid and encouragement, which has enabled me to get through this terrible time. To present my thesis to my whole family is a tremendous honor for me.

I also want to express my gratitude to my main supervisor, Lecturer Kavinga Yapa, who is a passionate and dedicated researcher who also happens to be an amazing mentor. Lecturer Kavinga Yapa is always ready to help me with any questions or concerns I have about my research, and it has been a pleasure working with him as a supervisor. I will be forever thankful to him for his encouragement and wise counsel. I had a fantastic experience on this academic journey and gained valuable research skills that will help me become a better researcher in the future.

In closing, I'd want to express my gratitude to all of my colleagues at SLIIT, especially those in the ISE department, for their efforts in fostering collaborative and lively discussion spaces.