Anonymous Traffic Network

Apurv Singh Gautam, Anushka Nagar, Rohan Nevrikar
Information Technology, Symbiosis Institute of Technology
Pune, India
apurv.gautam@sitpune.edu.n
anushka.nagar@sitpune.edu.in
rohan.nevrikar@sitpune.edu.in

***Abstract*-- Anonymity and privacy are the two major concerns of today's internet. Anonymous networks are poised to be an important service to support anonymous-driven Internet communications and consequently enhance user's privacy. Low latent anonymous communication networks, such as Tor, are inclined towards web browsing, instant messaging and other semi-interactive applications. Tor is now popular among dozens of thousands of Internet users. Tor is being widely used for P2P applications.**
In this paper we discuss about the onion routing concept and the feasibility and effectiveness of traffic through the Tor network. Furthermore, this paper provides the history of onion routing and the security issues related with the Tor network.
***Keywords*—Onion Routing, Anonymous Network, Nodes, Privacy, Internet, Monitoring, Protocols**

I. INTRODUCTION

Anonymizing networks such as Tor is being used more frequently by users that are aware about their anonymity or privacy. Tor was built with the main goal to avoid censorship from different countries and to allow them freedom of speech on the Internet. Anonymous communication (Tor) networks hide the actual source or destination address of Internet traffic which prevents the server or client and other entities along the network from determining the actual identities of the communicating parties. [1]

There are many Internet access restrictions policies deployed by the law enforcement which seems to push more and more users throughout the world to support Tor by setting up onion routers and exit nodes. In Tor, clients establish circuits through a chosen set of proxies which begins with an entry node and reaching the final destination through an exit node.

II. HISTORY

In 1995, David Goldschlag, Michael Reed and Paul Syverson started the research on Onion Routing. Their main aim was to separate identification from routing. Authentication of someone's identity can be done by the data which is sent through the network and it need not be done through one's location. The objective was not to create complete anonymity when browsing the Internet, but anonymous routing. [2]

The first formal publication on onion routing was released by mid-1996. In October 2003, the Tor network was launched and Tor code was made available for free under a license from MIT. By the end of 1996, about a dozen Tor nodes were set up by volunteers in US and Germany. By the end of 2004, there were over 100 Tor nodes on over 3 continents. By 2011, Tor nodes grew up to 2000 worldwide. [5]

In today's time, there are over 6000 Tor relays inside the network, serving over 1.5 million users. Many users such as the military, journalist, law enforcement officers, activists and others use Tor for different purposes and to benefit from the anonymous network.

III. OVERVIEW of ONION ROUTING

Onion routing is a technology aiming to provide anonymous communication between entities on a network. The goal is to provide low latency connections transparent to the end user, while the information exchange still is resistant against traffic analysis and other attacks. This is achieved by a set of encrypted layers and frequently changing paths between a subset of the routers that participates in the routing system. [4]

Onion routing is a technique for anonymous communication over a computer network. In an onion network, messages are encapsulated in layers of encryption, analogous to layers of an onion. The encrypted data is transmitted through a series of

network nodes called onion routers, each of which "peels" away a single layer, uncovering the data's next destination. The message arrives at its destination only when final layer is decrypted. The sender remains anonymous because each intermediary knows only the location of the immediately preceding and following nodes.

As you can see, the multiple layers of encryption make it really hard to break into your data packets. It's like a vault in which different other vault resides, even if you break into one, you still have to break into all of the rest.

IV. TRAFFIC & ROUTING

Circuit setup

For sending data through Tor network, a circuit has to be set up from the source (entry point). Randomly a circuit ID is chosen, a key exchange is initiated between entry point and the first hop. Key exchange happens between entry point and the first hop using Diffie-Hellman key exchange, a symmetric session key is negotiated. [4] Entry point sends request for extending the circuit, also having the new node, to the first hop. The circuit is extended to second hop by repeating the same process. At each node, the messages are encrypted using the negotiated session key, or if session key is not available then onion key of the receiving host is used.

Traffic through TOR network

Circuit is required to relay data. The information is encrypted in a lot of layers same as an onion, hence the name Onion Routing. Data to be sent is kept at the core along with other routing information which is to be sent to the exit node. The core is encrypted to be sent to the router which is nearest to the exit node having the information about the exit node. The same procedure is repeated for each router in the network. Each router decrypts the routing information of the next hop but it is unable to see from where the data is coming from or what is its destination or the data that is encrypted within. Not a single node in the path can determine what the data is and the exit node has no information about where the data has originated from. [4]

In previous versions of onion routing, there was a risk of any opponent installing a high performing router that could corrupt all the data. Tor was designed in such a way that it carries out integrity checking on the data sent through the network by using cryptographic hash functions at the end points and if corrupted data is found, the network can be changed.

Tor has a signalling scheme which can be used to change exit nodes which makes it virtually impossible to track changes in the circuit. This information if available can cause attacks on the network. For congestion control, signalling scheme is used.

Hidden Services

Web services are prone to DDoS, spoofing and various physical attacks. [4] To resist such attacks even from those who have authorized access to the service, one can hide both the logical and physical location of the service. Tor has a special feature known as Hidden Services which is used to hide the location of the service operator from the users and also hide the users from the operator. The question here is, how can a server which is publically accessible, hide its location on the network as well as its physical location? For this purpose, Tor uses a concept called rendezvous points.

Service operator can set up a hidden service such as a web server by generating a public/private key and selecting a number of onion routers (introduction points) which are used to set up tunnels. Service is announced on Service Lookup Server along with the public key. If a user wants to access this service, he/she finds an introduction point through Service Lookup Server and also chooses a router as rendezvous point to which tunnel is set up. The introduction point is informed about the rendezvous point and then it forwards this information to the service owner. To fully establish the connection between user and service, the service provider sets up a tunnel to the rendezvous point. Public key cryptographic method is used to secure the exchanges.

V. SECURITY ISSUES

Although data is encrypted along each of the relay nodes, it decrypts at the final node or exit node, and the path from exit node to the destination is unprotected if the requested site does not use SSL.

The exit node can potentially monitor the user's internet activity, keeping track of pages that the user visited. Another problem with using Tor is that if the user's machine is compromised by malware, then the user's identity is no longer anonymous. [4] Such a piece of malware called Magneto was discovered which exploited an

unknown vulnerability in the Tor browser which is commonly used to visit websites using Tor.

VI. TRACING of ANONYMOUS NETWORK

The Tor network does not provide bullet proof anonymity & confidentiality. The traffic from the exit node can be in plain text till the final destination which means that the confidentiality is at stake. [4] There are some attacks that can reveal the identity of a Tor user up to some extent. The main attack is timing analysis by watching packets leaving a user and entering a target server which can be correlated and probable user can be guessed.

Tunnels in Tor are reused by different applications. One can observe a traffic at an exit node and can correlate different traffic streams that can give some information about users.
There is also a way to attack user's anonymity which can be carried out with Java applets.

ActiveX control program can collect local information and send it back to the website owner which can be sued to gain user information.
Another way of tracking users is by IP traceback which can be used to find the origin of anonymous traffic. It can be deployed if there is a cooperation between Internet Service Providers (ISPs). [3]

REFERENCES

1. Abdelberi Chaabane, Pere Manils, Mohamed Ali Kaafar, "Digging into Anonymous Traffic: A Deep Analysis of the Tor Anonymizing Network" IEEE Publication http://ieeexplore.ieee.org/abstract/document/5636000/
2. Takuya Fukui, 02 February 2017, "Anonymous Routing of Network Traffic using Tor" https://witestlab.poly.edu/blog/anonymous-routing-of-network-traffic-using-tor/
3. Guang Yao, Jun Bi, Zijian Zhou, 30 September 2010, "Passive IP Traceback: Capturing the origin of anonymous traffic through network telescopes" ACM Publication http://dl.acm.org/citation.cfm?id=1851237
4. Henrik Erkkonen, Jonas Larsson, Datateknik, "Anonymous Networks: Online Routing with TOR, Garlic Routing with I2P" http://www.cse.chalmers.se/~tsigas/Courses/DCDSeminar/Files/onion_routing.pdf
5. OWL Cybersecurity, 01 September 2016, "Darknet Series: A Brief History of Tor" https://www.owlcyber.com/blog/2016/8/30/darknet-series-a-history-of-the-darknet