ISSN:2231-0711

Neha Singh et al | IJCSET(www.ijcset.net) | 2018 | Volume 8 Issue 2, 8-9

Securing Network communication over Web using Onion Routing

Prof. Neha Singh, Prof. Samruddhi Thawkar

Information Technology
SVPCET,Gavsi Manapur,Nagpur
Singhjass.singh@gmail.com
Samruddhi.thawkar@gmail.com

***Abstract*— In the modern era, all the devices are connected in the network via Internet. So, it becomes a major concern to protect data from surveillance I.e. monitoring of computer activity, data being transferred over computer networks such as Internet. So, we proposed Onion Routing Protocol to provide security over network, in terms of providing users their freedom and ability to conduct confidential communication by keeping their Internet activities from being monitored.**

***Keywords*— Security,Onion Routing,Anonymous.**

I. OBJECTIVE

The main focus is to have a network application which will allow different users to have anonymous communication with the help of onion routing which will provide resistance to several network security attacks like traffic analysis, eavesdropping,DOS (denial of service attack), man in the middle attack, replay attack etc.

II. INTRODUCTION

Due to the growth in the usage of internet one of the important need of today era is to secure the communications between different users from several kind of network attacks .In this paper we focus on two crucial network security attacks which are eavesdropping and traffic analysis. In eavesdropping the attacker attempts to listen the electronic conversations ,even if you try to secure messages by encrypting them encrypted they can be tracked using traffic analysis thereby revealing sensitive data and the identity of users involved in communication. Therefore the main aim of this paper is to analyze the concept of onion routing . Onion Routing is a general-purpose infrastructure to support private and anonymous communication [1] over a public network.

III. WORKING OF ONION ROUTING

There are different routing srategies that are used for routing the information from source to destination.The main focus of Onion Routing[2] is to Provide security to communication being held between two users over internet. The essential element in onion routing is the routing onion. Which can be considered as the data structures used to create different paths through which multiple messages can be transmitted.

Steps to To create an onion

- The Client sends the request to Onion Proxy which selects random number of onion routers from the Routers Cloud to form layers of onion.
- The onion will have layers comprising of Data,Private keys,IP Addresses of Routers. for decryption to find the next router Ip address in the path to reach the destination (Target System) .
- The messages to be forwarded are encrypted by the router's public key which provides a layered structure.
- As soon as the router receives the message, it decrypts it with its private key therby peeling a layer from the onion .

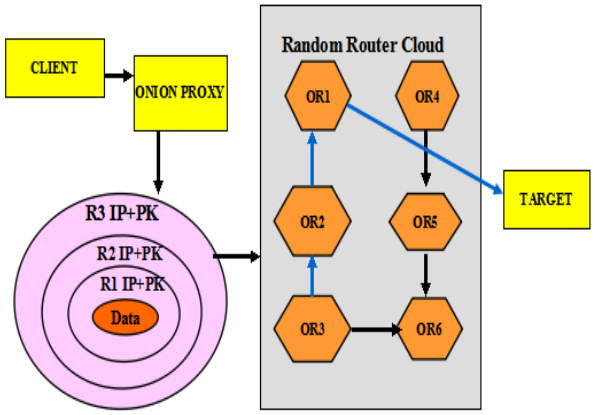

Fig. 1 Architecture of Onion Routing

In the fig(1) notations used are OR-Onion router
IP- ip address
PK- Private Key
R- Router

- Peeling of layers of Onion is done until its last layer ,when the data is found it transmits the data in the Onion to the intended Target System.

L(Rd)----------->Z(IP) +E ----------Equation (1)

where, **L-Layer**

R-Router
D-Decryption
Z-Next Random Router
IP-Ip address
E-Encrypted Data
PK-Private Key

Due to selection of random router the probability of the same path selection for transmitting the message from client to target system will be very rare and hence traffic analysis[3] and Eavesdropping can be overcome by this Onion Routing technique.

IV. FUTURE SCOPE

Onion Routing [4] is mechanism to provide anonymity to the users involved in communication and provide security from eavesdropping and traffic analysis attack. It is the process in which the sender (initiator) and the receiver (responder) nodes communicate with each other anonymously by means of some intermediate nodes called as onion routers. Data to be exchanged is encrypted by public keys of routers and decrypted by private or session keys of routers which results in overhead. We will try to reduce the overhead involved in encryption decryption process by using some cryptographic algorithm. Moreover will try to improve the performance of onion routing by using some path selection methods or relevant routing techniques that will be secure and efficient .

V. CONCLUSION

Security is an important aspect of communication over the web.Hence it becomes very essential to mitigate traffic analysis. Onion routing is by far the best solution for maintaining anonymity over the web. In onion routing (for wired networks) data is wrapped under multiple layers of encryption and forwarded towards the destination and each node on the route decrypts a layer and forwards it. But certain modifications need to be made while applying onion routing on the wireless network.

REFERENCES

[1] Michael G. Reed, Paul F. Syverson, and David M.Goldschlag "Anonymous Connections and Onion Routing" IEEE JOURNAL ON SELECTED AREAS IN COMMUNICATIONS, VOL. 16, NO. 4, MAY 1998

[2] K.Kaviya, "Network Security Implementation by Onion Routing" IEEE 2009 International Conference on Information and Multimedia Technology

[3] Paul Syverson, " Onion Routing for Resistance to Traffic Analysis" Proceedings of the DARPA Information Survivability Conference and Exposition(DISCEX'03) 2003 IEEE

[4] Qiang Fang, Songmei Liu, Ruijin Zhou, "The Application of Onion Routing in Anonymous Communication" , 2010 IEEE