IJIRSET
International Journal of Innovative Research in
SCIENCE | ENGINEERING | TECHNOLOGY

e-ISSN: 2319-8753 | p-ISSN: 2347-6710


# INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

## IN SCIENCE | ENGINEERING | TECHNOLOGY

Volume 10, Special Issue 2, December 2021

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

Impact Factor: 7.569

9940 572 462 | 6381 907 438 | ijirset@gmail.com | www.ijirset.com

International Journal of Innovative Research in Science, Engineering and Technology (IJIRSET)

|| e-ISSN: 2319-8753, p-ISSN: 2320-6710| www.ijirset.com | Impact Factor: 7.569| || Volume 10, Special Issue 2, December 2021 ||

4th International Conference on Emerging Trends in Science, Technology and Mathematics [ICETSTM '2021]

15th & 16th September 2021

Organized by

Department of Computer Science, Parvathy's Arts and Science College, Dindigul, Tamilnadu, India

# De- Anonymizing Tor Hidden Services

**T.Gayathri[1] , Dr.A.Saraswathi[2]**

Assistant Professor, Department Computer Science, Govt. Arts College, Trichy, Tamil Nadu, India [1]

Assistant Professor, Department Computer Science, Govt. Arts College, Karur, Tamil Nadu, India[2]

**ABSTRACT***:* A groups, workers, and ordinary persons may want to communicate through internet without disclose what they are or who they are doing .This can be done via the user of anonymous network protocols, their goals are to provide anonymity to the network user. Here onion routing is one such application which enables user to have anonymous communication. Tor support the hidden services to preserve the darkness of these web services. The hidden services are deducted in tor networks. Researchers are bothered about the different attacking schemes to deanonymize the hidden service. We propose cca technique to provide security to tor hidden services and minimize the deanonymization of the hidden service in a secured manner.

**KEYWORDS:** Tor, anonymity, hidden services, de-anonymization

## I. INTRODUCTION

Research is low visibility anonymity network has mostly absorbed on sender anonymity allowing users to assassociate to network resources without disclosing their network address to the destination. In onion routing ,instead of introducing a direct transmission between the two host that want to transmit the closeness will be directed through a set of routers called onion routers and hence allow the transmission to be anonymous. [1] we do not want the third party to know the person with whom we are transmitting onion routing[2] is basically associated with a set of proxies which help in transmission. The creator first establish an creator transmission with application proxy on his or her machine through which the transmission are routed to the onion proxy which define the route to the destination and consult the onion. The data structure will be commute between the node crowds[3] is another anonymous protocol which is same in operation to onion routing. The differenced dispute are in the encryption scheme and in the path selection. The paths are select dynamically as a message is set, rather than setting up a circuit as onion routing does. Responder privacy can bee achieved with tor by making TCP service accessible as hidden services. We look at them from different attack viewpoint and provide a structured picture of what information can be obtained with very inexpensive means. We focus on both attaks that allow edit access to choose hidden services as well as on deanonymization of hidden services. The hidden services are website located inside th TOR network which receive inbound connection only through Tor. The deanonymization need the opponent manage the tor entry point for the computer hosting the hidden service. It also need the attacker to have already collected unique network character that can serve as a fingerprint for that exacting services. Tor officials say the need reduce the success of the attack still the new analysis underline the limits to anonymity on tor which journalists,activists and criminals alike relay on to void online observation and monitoring.
Classifier algorithm that allowed the examination to recognize certain traffic as belonging to a tor hidden service. It has three phases

- The hope to get happy and end up running the entry guard for the tor user they are trying to traget.
- The traget user load some webpage using tor and they use a classifier to guess wheather the web page was in onion –space or not.
- Lastly if the first classifier said yes it was they use a separate classifier to guess which onion site it was.
- Deanonymizing hidden service is the design in which ip address of anonymous website is reveled. one way to deanonymize these hidden services is by attacking them in different manner.

## II. THE TOR BROWSER

The onion routing browser may be a application plot for anonymous net surf riding and protection against traffic analysis. Tor is usually related to the dark net and criminal activity, enforcement, officials , reports, activists use the browser for legitimate reasons. The tor works by employing a technology called onion routing . The onion router is

|| e-ISSN: 2319-8753, p-ISSN: 2320-6710| www.ijirset.com | Impact Factor: 7.569| || Volume 10, Special Issue 2, December 2021 ||

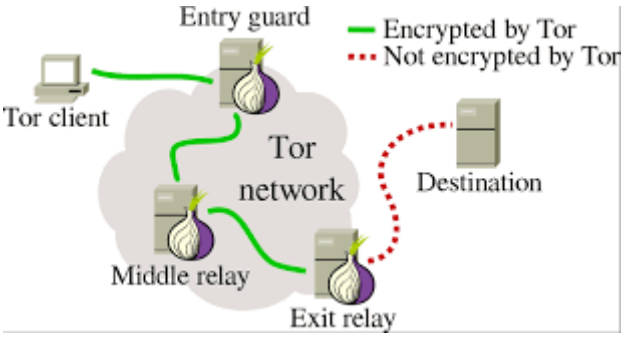
4th International Conference on Emerging Trends in Science, Technology and Mathematics [ICETSTM '2021]

15th & 16th September 2021

Organized by

Department of Computer Science, Parvathy's Arts and Science College, Dindigul, Tamilnadu, India

peer to look overlay network that permits users to browse the web anonymously. onion routing uses multiple layers cryptography to hide each supply and destination of knowledge send over the network.
The browser user tor servers to send information to an exit node that is that the purpose at that information leaves the network. once this information has been sent it's encrypted multiple times before being sent to subsequent node. Redo this activity makes it difficult to trace the info back to the first supply.




The network of the tor has a three components to anonymously connect a user to server on the networks. Their are relays,exit relays, and directory servers.

Relays:

The most common type of server make use of the tor network. It can be run by anyone ready to run the tor software. This servers only send traffic inside the tor networks and as such are not at all used to attack out of the network to the internet.

Exit Realys:

Exit relays execute as relays but also send on traffic inside the Tor network to the outside internet. Each exit relay has connected their own policy which specifies which kind of trafffic the relay is ready to forward out of the network and to which networks.

Directory Servers:

This server is a center part of the onion router network. This servers are authority for collecting a list of active relays in the network and bring the public keys essential for client to establish protected connections to them.The address of the directory server is involve in the distributed Tor software across the public key of each directory server. This is the same for relays which will promote their availability and statistics to the directory servers in order to be list accordingly. The Directory servers will then construct a consensus regarding the state of the network between themselves. Once this consensus is reached the result is endorsed by the directory servers and give out to relays ready to catch the directory consensus. To escape constitute single points of failure in the network design, directory servers are not completely trusted. Alternatively clients and relays will prove the signatures of the consensus to make sure that a minimal half of the directories agree on its contents by deliver their own trusted directory, servers as the code that operate the clients relays and directories is completely open source.

## III. TECHNICAL DESCRIPTION

3.1 Onion Routing

Basically integrated with a set of proxies which help in transmission. The originator first establish an initiating connection with application proxy on machine via which the transmission are routed ot the onion proxy which define the route to the receiver and build the onion the data structure that will be travel between the nodes. onion proxy initiate the connection with the first node in the route and move on the onion to.

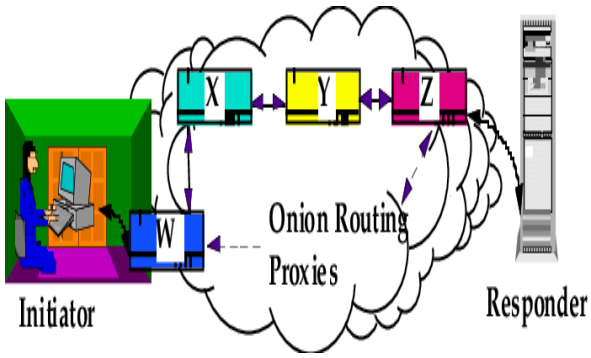
|| e-ISSN: 2319-8753, p-ISSN: 2320-6710| www.ijirset.com | Impact Factor: 7.569| || Volume 10, Special Issue 2, December 2021 ||

4th International Conference on Emerging Trends in Science, Technology and Mathematics [ICETSTM '2021]

15th & 16th September 2021

Organized by

Department of Computer Science, Parvathy's Arts and Science College, Dindigul, Tamilnadu, India




which basically stripes of a layer of onion to get information about the next node on the route and therefore modify the onion and send it to the next router.

3.2 Proxy Redirection

The internet proxy is a server that send on data from a sender to a specified concrete recipient and also forwards reply from the recipient back to the sender. A proxy may be used to bring limited anonymity to the sender. When the receiver checks the identity of the source he sees the proxy instead fo the original sender. The proxy is a single point of loss in this system and so an attacker may totally compromise the anonymity of the sender by achieve control of the proxy or simply analysing traffic in and out of it.

3.3 Public key Cryptography

This cryptography any participant has two keys that can be used for meassage encryption and decryption.. source key is public and the destination key is private. Public keys are easily accessible from online registry called key servers. The unique cryptography is done by the related public and private keys.

3.4 Symmetric Keys

Symmetric key can be achieved faster encryption These are commonly quite short relative to the information they encrypt however and therfore it is empricial to safe guard the transportation of symmetric key negotiations using public key cryptography.

## IV. HIDDEN SERVICES

Is a server that transmit completely with clients using the tor network. In addition to bring the related routing anonymity as for clients, tor contain a machanism for permit the hidden services ot preserve a constant name or URL address. Although achieving the hidden service will quit need to building circuits, a client request to attain a hidden service will not demand the make use of an exit relay. Absolutely two added types of relays are need to hide the client and hidden service from one another efficiently. one is introduction points second is rendezous points.

## V. PROBLEMS AGAINST TOR HIDDEN SERVICES

Tor is safer than most typically used browsers. it's not impermeable to attack whereas tor protects against traffic analysis it doesn't forestall finish to finish correlation.

Consensus blocking – the tor exit relay is vulnerable to category of attacks that permits a malicious user to briefly block accord nodes from communication.

Denial of service(dos) attack that blocks access to an internet site by flooding it with such a large amount of requests that it's not possible for the servers to stay up

Eves dropping because the traffic passing through doesn't use E2EE. during this methodology doesn't expressly reveal a users identity, the interception of traffic will expose data concerning the supply.

Traffic analysis attack in passive traffic analysis attack an interloper extracts data and matches that data to the other facet of the network. In active attack the interloper modifies packets following pattern to assess their impact on traffic.

Sniper attack overwhelms exit nodes till they run out of memory. An attacker can decrease the number of operating exit nodes, increasing the probability of users using exit nodes force by the attackers.

|| e-ISSN: 2319-8753, p-ISSN: 2320-6710| www.ijirset.com | Impact Factor: 7.569| || Volume 10, Special Issue 2, December 2021 ||

4th International Conference on Emerging Trends in Science, Technology and Mathematics [ICETSTM '2021]

15th & 16th September 2021

Organized by

Department of Computer Science, Parvathy's Arts and Science College, Dindigul, Tamilnadu, India

## VI. ATTACKING STRATEGY

Hidden service offers a transmission anonymity for a constant service. Users are able to associate to the service between Tor without knowing its location. These hidden services can provide the illega websites whose effect can be severe. so these HSS need to be betray. Deanonymizing hidden service is the program in which ip address of anonymous websites is revealed. one way to deanonymize these hidden service is by attacking them. The researchers till now have developed so many different attacking schemes.

- All attacking schemes need adversary client and adversary guard node to denanymize hidden service.
- They are mandatory to choose the endangered guard nodes as their entry nodes.
- They reveal the ip address of hidden systems.

Table 1 mention about the different types of attacks and how they are affecting the tor hidden network environment.

Table 1

| Attack | Issues |
|---|---|
| Traffic Analysis | It does not prevent end-to end correlation and modifies the packets. |
| Consensus Blocking | Malicious user to temporily block consensus nodes. |
| Denial of service | Which blocks access to a website by flooding it with so many requests . |
| Eavesdropping | The interception of traffic can expose information about the source |
| Sniper Attack | Attacker can reduce the number of functioning node and control the exit nodes. |

## VII. RELATED WORKS

The attacker [4] [5] periodically sends a large amount of data to the hidden server through the TOR client, which will increase the temperature of its CPU, resulting in a clock skew pattern, and remotely measure the clock law of a group of candidate systems and try to detect matching patterns to de-anonymize the hidden services.
The trawing, Tor services attacker can regulate access to HS descriptors, hidden service movement can be observed or be fully in accessible to client. [6], discussed how information leaks in the layout or content hosted on Hss can be used to disclose their location reviewed a considerable number of onion sites for URLs. [7] [8], point out that if an attacker control the position itself as a false HsDir, it can cause an eclipse attack for denial of service attacking decentralised networks.

## VIII. CONCLUSION

The aim of onion routing is to keep the anonymity of a client who want to transmit over a network. The outside viewers will not be able to describe whom th client is transmitting cryptography methods for maintaining secure transmission. we want to extent this and minimize the threats. A deeper determination of the attack is consider and their degree of success of failure can be made estimate how the tor project has closed vulnerabilities that multiplex of these attacks utilized.

|| e-ISSN: 2319-8753, p-ISSN: 2320-6710| www.ijirset.com | Impact Factor: 7.569| || Volume 10, Special Issue 2, December 2021 ||

4th International Conference on Emerging Trends in Science, Technology and Mathematics [ICETSTM '2021]

15th & 16th September 2021

Organized by

Department of Computer Science, Parvathy's Arts and Science College, Dindigul, Tamilnadu, India

## REFERENCES

[1] Michael g. reeed, Paul F. Syverson, and David M.goldschlag Anonymous Communications and Onion Routing, IEEE Journal 1998

[2] Roger Dingledine, Nick Mathewson and Paul syverson, Tor: The second generation Onion router. 13th USENIX Security Symposium,2004

[3] The Anonymizer, http://www.anonymizer.com

[4] Murdoch,S.J.Hot or Not: Revealing Hidden Services by their Clock Skew Categories and Subject Descriptors,13th ACM conference on Computer and communications security,2006,pp.27-36

[5] Panchenko,a.;Mitseva,A.;Henze,M.;Lanze,F.;Wehrle,K.;Engel,T.Analysis of Fingerprinting Teschniques for Tor Hidden Services.Proceedings of the 2017 on Workshop on Privacy in the Electronic Society

[6] Zander,S.;Murdoch,s. An Improved Clock-skew Measurement Techique for Revealing Hidden Services,USENIX security symposium 2008,pp.211-225

[7] Tan,Q.;Gao,Y.;Shi,J.;Wang,X.;Fang,B.;Tian,Z.oward a comprehensive Insight Into the Eclipse Attacks of Tor Hidden services, IEEE Internet of Things Journal 2019.

[8] Tan,Q.;Y.;Shi,J.;Wang,X.;Fang,B.; A closer look at Eclipse attacks against Tor Hidden Services. 2017 , IEEE International conference on communications.

[9].“Announcing the vanguards add-on for onion services.” [Online].Available :https://blog.torproject.org/announcing-vanguards-add-onionservices.

INNO SPACE
SJIF Scientific Journal Impact Factor

Impact Factor:
7.569

doi cross ref

ISSN INTERNATIONAL STANDARD SERIAL NUMBER INDIA

निस्केयर NISCAIR

# INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

## IN SCIENCE | ENGINEERING | TECHNOLOGY

9940 572 462 6381 907 438 ijirset@gmail.com



Scan to save the contact details