ISSN 2348 – 8034
Impact Factor- 3.155

GLOBAL JOURNAL OF ENGINEERING SCIENCE AND RESEARCHES

ALLOWING GENUINE USERS AND BLOCKING MALICIOUS USERS IN ANONYMIZING NETWORK: THE NYMBLE

Mr. Anand A. Maha[*1] and Assoc. Prof. P. B.Kumbharkar [2]
[*1]Student, Computer Engineering, Siddhant College of Engineering Sadumbare, Pune, India
[2] Assoc. Prof. P. B.Kumbharkar, Computer Engineering, Siddhant College of Engineering Sadumbare, Pune, India

ABSTRACT

Network is a combination of client server architecture which is responsible for information exchange. Network which avoid the sharing of users IP address and other information from server and routers is known as anonymizing network. However users are misusing popular websites using this network. Service provider of these websites or website owner can block such whole network. But if any honest user is reside inside that network then he will also be blocked by that website. The Owner will block all the existing users of the anonymizing network. And it will affect the anonymous access to the malicious nodes along with honest users. Nymble is a system which detect misbehaving nodes inside the anonymous network. We will use Nymble to block such malicious users and allowing access to honest users. Nymble will preserve privacy of malicious nodes of anonymizing network.

Keywords: *Anonymous blacklisting, Privacy, Revocation.*

I. INTRODUCTION

Number of internet users is increasing every day. As privacy preservation is a main issue on internet so no one wants to share their private information on internet. Private information may consist of user details, IP address, Location etc. Due to this users are trying to access the internet through anonymous network. For example TOR. TOR is an anonymous network which diverts traffic over Internet through a volunteer network. This network contains approximately five thousand and above relays to hide a user's identity and other information other monitoring users. It is very difficult to track user activity when user is inside the TOR network. Intension behind development of TOR is to preserve user privacy and provide freedom to user for confidential communication inside monitoring area.

.

As per above discussion, the TOR is capable for hiding identity of the user's and from the others location. So the user of TOR can capable to operate maliciously on several famous website like YouTube, Wikipedia. To this problem the existing system gives several solutions, using duplicate name called as pseudonyms, Pseudonymous systems users log into websites, if a user misbehaves on that site this pseudonym can be added to a blacklist. But, for all users this approach results in pseudonymity, and user which are inside the anonymous network, it blocks that all. The group of users creates the basic pseudonymous systems in which to the central manager every users can submit their complaint. For each authentication the server has to query to the group manager. So that the scalability of the network get reduced. The group manger opens the trapdoor to track the particular user. The subjective blacklist is maintained by every server in which all the misbehaving users are added. So that, the users are remain private which have names of the blacklisted.

The server about one millisecond per authentication taken by the VLR. So that our system is several thousand times faster than VLR. When weighed against the potential benefits of anonymous publishing, we believe these low overheads will incentivize servers to adopt such a solution.

The procedure of destroying the electronic trail or tracts is the data anonymization, on the data, to its origins that would show the way to an eavesdropper. To anonymizing Internet communications anonymizing networks for example Tor or I2P provides a strong way, so that to link communication parties it will be very hard. Over the time in anonymizing networks there are several forms of credential systems evolved. To resolve the actual and important problem of permitting users, anonymous communications networks facilitate to communicate privately over the Internet.

ISSN 2348 – 8034
Impact Factor- 3.155

Literature survey

By blocking IP addresses of abusers many existing services limit user abuses like posting spam or inappropriate comments, or when creating a user account, requiring users to prove ownership of a valid email address, if the user misbehaves which can then be disabled. While such measures does not consider by the academic literature to be strong deterrents, as a trade-off between the needs of servers to limit abuse they are nevertheless widely implemented, and the reluctance of users to maintain cryptographically strong digital identities or provide sensitive identity information (like bank or government identifiers) just to post a blog comment or edit a Wikipedia article.

A. NYM System.

To allow pseudonymous access to Internet services via anonymizing networks like Tor NYM is an extremely simple way, to limit vandalism using popular techniques such as blocking owners of offending IP or email addresses without losing the ability. To create a pseudonymity system with extremely low barriers to adoption NYM uses a very straightforward application of blind signatures. To pseudonymously obtain a blinded token Clients use an entirely browser-based application for an ordinary TLS client certificate which can be anonymously exchanged.

On the Tor email list about Wikipedia's practice of blocking Tor users from making changes to articles NYM grew out of a discussion. Due to abusers who had used Tor in the past Wikipedia blocks most Tor exit nodes to avoid IP-address based bans. There mentioned the Privacy protecting credential systems, but it was pointed out that such systems tend to be patent-encumbered and difficult to implement. Another problem was the basis for pseudonymity; in terms of large, established agencies issuing digital credentials to the masses, privacy protecting credential systems are generally described. A high-stakes game of cryptographically certified personal information create by such systems to intimidate users of an anonymity network like Tor which would naturally tend [3].

B. Credential System:

Users can obtain credentials from organizations and reveal possession of credentials which is a credential system. When transactions carried out by the same user cannot be linked this system is called anonymous. Anonymous credential system consists of users nothing but clients and respective organizations. Only by user's pseudonyms these organizations know the users. The basic system contains protocols. To join the system these protocols are used by user, and then to register with an organization and then, retrieve multiple show credentials, and display that credentials.

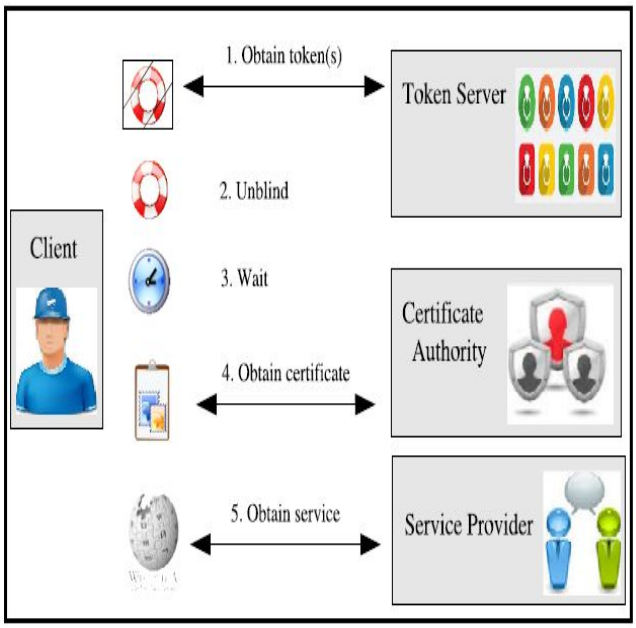

Figure 1. NYM System Architecture.

ISSN 2348 – 8034
Impact Factor- 3.155

C. PEREA:

Privacy-Enhanced Revocation with Efficient Authentication (PEREA), it is an authentication method which does not require TTP. In this the time complexity of PEREA at the time of bottleneck operation is independent on blacklist size. Here computation used is linear and it is having size K times of the revocation window, It detects the number of false authentication and blacklists that misbehaving user before its revocation process.

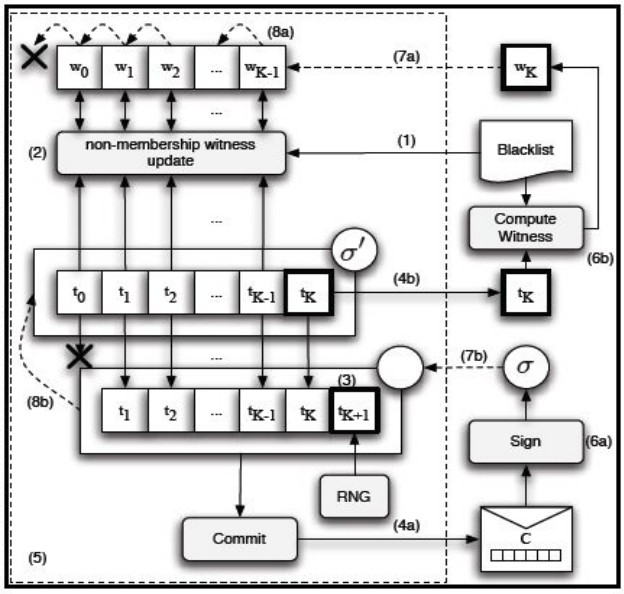

Figure 2. PEREA System Architecture

II. PROPOSED SYSTEM

The Nymble, possesses the characteristics like: quick authentication, unlink-ability to backward operations, blacklisting basis of subjective methods, rate-limited connections and malicious authentication detection. Initially the web user get connected to Nymble. After connecting Nymble generates pseudonym for user. User users that pseudonym to connect with server.

Normally the website service provider blocks the malicious user by gaining seed of a Nymble. If in future that malicious user tries to use services of user then server will obtain its seed from Nymble, check that seed in blacklists users, if user found then it will directly blocked again without knowing actual IP address of user. Such blacklisted users are disconnected immediately by Nimble. Nymble can access any number of user at a time and process their seeds.

The Figure 3 gives the system architecture of the Nymble System. It consist of 3 modules,

1. User.
2. Pseudonym Manager.
3. Nymble Manager.

ISSN 2348 – 8034
Impact Factor- 3.155

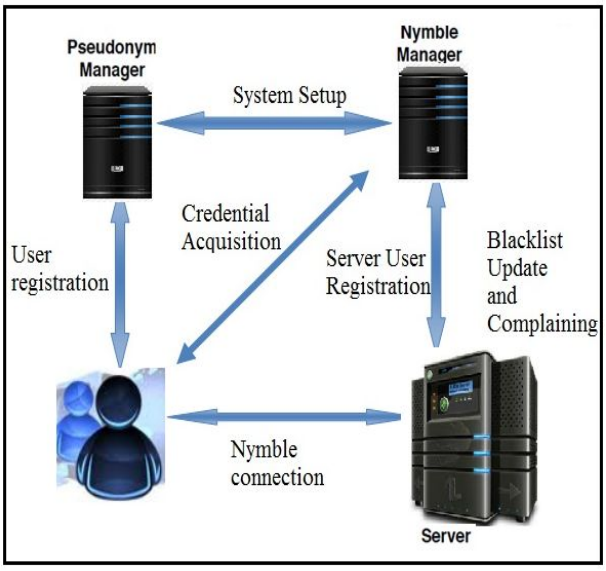

Figure 3. System Architecture.

Our system provides the means by which server can easily blacklist the malicious user in the anonymous network. Also our system provides protocol to do the cryptographic operations.

1. *User:*

User is anyone who wants to use anonymous network. User may be of two types, first one is honest user and another one is malicious user who is misbehaving in network. User can use pseudonyms inside the synonymous network if it is connected via Nymble.

2. *Managing the Pseudonyms.*

Before using actual resources user must connected to pseudonym manager (PM). Overall management of pseudonym is done by PM. It assigns fake name to user resources. Then PM generates Resource- pseudonym pair for individual user. PM does not maintain any record about website user id going to use this resources.

3. *Nymble Manager:*

After PM user connects to Nymble Server. After that by making use of pseudonym user can able to access the website via anonymous network. Nymble system generates a server-pseudonym pair. This pair is wrapped inside the tickets or seeds generated by Nymble. Encapsulation will serve cryptographic approach for improvement in security parameters. Every Nymble ticket is bind with time span. If time span is less then it provides quick authentication. Authentication of user will be done once for whole day.

4. *Blacklisted Users.*

During authentication in Nymble If any user behaves maliciously then it is added to the Blacklist. After adding user into black list server will generate complaint link and attach it with user seed and resources and forward it to Nymble manager (NM). At NM Nymble ticket of that user will selected and it will send back to server.

III. RESULT & DISCUSSION

Blocking misbehaving users inside anonymous network is main aim of our system. How the particular IP address is blocked has been shown in the figure 4. The system displays the information that the particular IP address has been blocked because of the misbehaving details shown in the message. One key feature is that the Nymble server show the wrong password entered by the misbehaving user so that he will get aware that someone is watching what he is entering as password.

ISSN 2348 – 8034
Impact Factor- 3.155

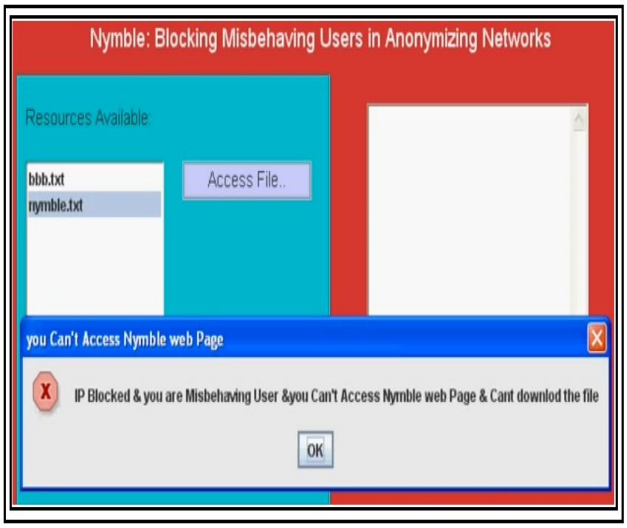

Figure 4. Blocking misbehaving user.

After blocking user Nymble Server provides misbehavior report to Nymble Manager.

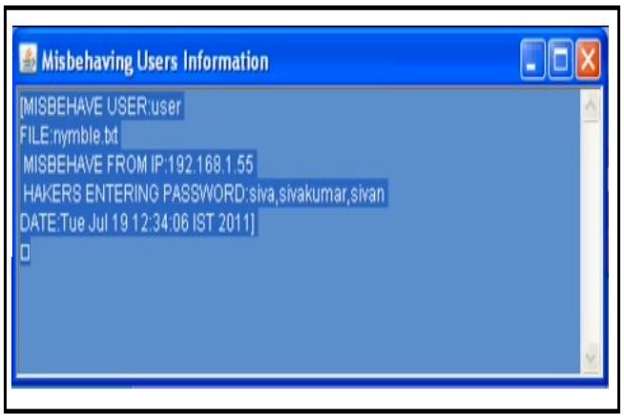

Figure 5. Misbehavior report sent by server to NM.

IV. CONCLUSION

Here we come to conclude that Nymble can used effectively to avoid misuse of pseudonymity inside the anonymous network. Nymble preserves anonymity of users which is very essential in anonymizing network. Nymble can be used as a part of security inside the most popular websites or network where system admins or website owners used to blacklists the misbehaving users as the Nymble is effective system against malicious behavior.

V. ACKNOWLEDGEMENTS

We would like to take this opportunity to express our profound gratitude and deep regard to my Guide Prof P.B. Kumbharkar, for his exemplary guidance, valuable feedback and constant encouragement throughout the duration of the project. We would also like to thanks to Principal, Siddhant College of Engineering Sadumbare. We are also thankful to our family and friends for their encouragement and support.

ISSN 2348 – 8034
Impact Factor- 3.155

REFERENCES

1. *Patrick P. Tsang, Apu Kapadia, Member, IEEE, Cory Cornelius, and Sean W. Smith "Nymble: Blocking Misbehaving Users in Anonymizing Networks" Digital Object Indentifier 10.1109/TDSC. IEEE 2009.*
2. *S. Goldwasser, S. Micali, and R. L. Rivest. A Digital Signature Scheme Secure Against Adaptive Chosen-Message Attacks. SIAM J. Comput., 17(2):281–308, 1988.*
3. *J. E. Holt and K. E. Seamons. Nym: Practical Pseudonymity for Anonymous Networks. Internet Security Research Lab Technical Report 2006-4, Brigham Young University, June 2006.*
4. *P. C. Johnson, A. Kapadia, P. P. Tsang, and S. W. Smith. Nymble: Anonymous IP-Address Blocking. In Privacy Enhancing Technologies, LNCS 4776, pages 113–133. Springer, 2007.*
5. *A. Kiayias, Y. Tsiounis, and M. Yung, "Traceable Signatures," Proc. Int'l Conf. Theory and Application of Cryptographic Techniques (EUROCRYPT), Springer, pp. 571-589, 2004.*
6. *A. Kiayias, Y. Tsiounis, and M. Yung. Traceable Signatures. In EUROCRYPT, LNCS 3027, pages 571–589. Springer, 2004.*
7. *B. N. Levine, C. Shields, and N. B. Margolin. A Survey of Solutions to the Sybil Attack. Technical Report Tech report 2006- 052, University of Massachusetts Amherst, Oct 2006.*
8. *A. Lysyanskaya, R. L. Rivest, A. Sahai, and S. Wolf. Pseudonym Systems. In Selected Areas in Cryptography, LNCS 1758, pages 184– 199. Springer, 1999.*
9. *S. Micali. NOVOMODO: Scalable Certificate Validation and Simplified PKI Management. In 1st Annual PKI Research Workshop - Proceeding, April 2002.*