NYMBLE: Denying Access To Misbehaving Users In Anonymizing Network

Aditi R. Raut, Gaurav S.Wagh, Sejal R. Zade,
Prof. Raminder Kaur
Department of Information Technology
Atharva College of Engineering, Malad (W), Mumbai-400095
Email: aditiraut16193@gmail.com , gauravwagh16193@gmail.com , zadesejal@gmail.com , raminder12_kaur@yahoo.co.in

Abstract – **In today's world internet has become a vital part in everyone's life. Internet has its own impact on an individual and society, but privacy is a major issue. Network is "collection of connections". Anonymizing network such as TOR [5]allow users to access internet services privately using a series of routers to hide the client's IP address from the server. TOR's success, however, has been limited by users employing this anonymity for abusive purposes, such as defacing the website. Wikipedia –is one of the example of defacement of website. Website administrators rely on IP address blocking for disabling access to the misbehaving users , but this is not practical if the misbehaving user routes through TOR. As a result, administrators block all the TOR exit nodes denying anonymous access to honest and dishonest users alike. To address this problem, we present a system in which:**

(1) Honest users remain anonymous and their requests unlinkable.

(2) A server can complain about a particular anonymous user and gain the ability to blacklist the user for future connections.

(3) User's are aware of their blacklist status before accessing a service.

As a result of these properties, our system is resistant to different servers' definitions of misbehavior.

I. INTRODUCTION

Anonymizing networks such as CROWDS and TOR route traffic through independent nodes in separate administrative domains to hide the originating IP address. Unfortunately, misuse has limited the acceptance of deployed anonymizing networks. The anonymity provided by such network prevents website administrators from blacklisting individual malicious user's. IP addresses; to thwart further abuse, they blacklist the entire anonymizing network. Such measures eliminate malicious activity through anonymizing networks at the cost of denying anonymous access to honest users. Websites used an assigned pseudonym (ticket), thus assuring a level of accountability. Unfortunately, this approach results in pseudonymity for all users—ideally, honest users should enjoy full anonymity, and misbehaving users should be blocked. To this end, we present a secure system in which users acquire an ordered collection of nymbles , a special type of pseudonym, to connect to websites. Without additional data, these nymbles are computationally hard to link, and hence using the stream of nymbles simulates anonymous access to services. Websites, however, can blacklist users by obtaining a trapdoor for a particular nymble , allowing them to link future nymbles from the same user—those used before the complaint remain unlinkable. Servers can therefore blacklist anonymous users without knowledge of their IP addresses while allowing honest users to connect anonymously. Our system ensures that users are aware of their blacklist status before they present a nymble, and disconnect immediately if they are blacklisted. Furthermore, websites avoid the problem of having to prove misbehavior: they are free to establish their own independent blacklisting policies. Although our work applies to anonymizing networks in general, we consider TOR for purposes of exposition. In fact, any number of anonymizing networks can rely on the same Nymble system, blacklisting anonymous users regardless of their anonymizing networks of choice.

II. LITERATURE SURVEY

At present, there are various algorithms being implemented for network security. The following are research papers presented in order to achieve network security.

- Sybil Attack [1], J.R.Douceur: Large-scale peer-to-peer systems face security threats from faulty or hostile remote computing elements. To resist these threats, many such systems employ

redundancy.This algorithm traps attacker with different identities. Sybil attack is an attack when the attacker tries to attack the website using different identities.

- Group Signatures [4] [7], E.Breson and J.Stern: In group signatures various members can anonymously sign a message on behalf of the group. A group manager is in-charge of adding group members and has the abilityto reveal the original signer.
- nonymous Credentials[2], J. Camenish and A. Lysyanskaya: Web applications dealing with personal data in privacy friendly way have a need for anonymizing credentials. While protocols, libraries are available to implement such applications, credential computing cannot built a credential infrastructure and vice-versa. Initial cost is reduced for both the parties in the business.
- he Onion Routing [5], R. Dingledine , N. Mathewson and P. Syverson: It is a circuit based anonymous communication service. Address the limitations in previous design by perfect forward secrecy congestion control directory servers and integrity checking. It works on real world internet, requires more special privileges or kernel modifications. It provides a reasonable tradeoff between anonymity usability and efficiency.
- Pseudonym Credential System, R.Rivest, Kapadia: Credential System is a system in which the users are identified and authorized by a third party which is trusted. In Pseudonym Credential system the users are identified and authorized using pseudo-names(false names). This system eliminates the use of generation of public keys, private keys secret keys etc. which is a tedious process. This system uses encryption techniques and digitally signed certificates.
- Nymble: Blocking Misbehaving Users using IP Address[3], P.C.Johnson: In this system, misbehaving users usually try to deface a website or hack a system. These users use TOR or CROWDS to reach the destination website. Hence ,this system takes their IP Address and blocks the users on the basis of this information.

Hence different techniques and algorithms have been implemented to protect the networks and make them more secure. Although these improved algorithms and techniques can reduce number of error and improve the security but these too have some loop holes in them. Above papers shows that the existing system uses different algorithms or technologies for example, digitally signed certificates, encryptions and decryption techniques, generation of different keys, blocking based on IP Address etc. Therefore we are proposing a system in which we try to eliminate the above loop holes and limitations and provide a more secure and reliable system.

III. LIMITATION OF EXISTING SYSTEM AND IT'S LOWER VERSIONS

- To overcome the Sybil attack certificates are used. But validation of the certificates is a tedious work. If there are multiple certificates which are to be validated, the system crashes.
- In group signatures members sign in anonymously on behalf of the group. To reveal the original signer generation of secrete keys by the group manager is important. But generating this keys is difficult.
- In anonymous credential system the time is wasted, since anonymous authentication is done in friendly way.
- In TOR, if one node breaks down all its circuit connected to it must break. Therefore, the users abundant the system because of its brittleness. If the broken node is fixed after failure the assurance cannot be given whether the anonymity is lost or not.
- For blocking misbehaving users in anonymizing network, IP(Internet Protocol) was used. The misbehaving users would route through series of router in order to hide the IP address which was being blocked by the servers. Therefore the misbehaving users were able to access the server even if they were blocked.
- The honest users in the anonymizing network would be affected by the behavior of illegal users, since the server blocked the exiting nodes of the network.

IV.OVERCOME BY PROPOSED SYSTEM

- The NYMBLE system uses IP as well as MAC address in order to block the misbehaving users in anonymizing network.
- The user cannot posses multiple identities due to MAC address. Hence Sybil attack is prevented.
- Tickets are generated based on the host name present in IP address. These generated tickets provide the means of authentication between the servers.
- The use of certificates and credential systems are avoided.
- Subjective blacklisting is provided i.e., the servers can have their own blacklisting policies.
- The system provides quick and real time response.
- The timestamp of one day is issued if the user misbehaves.

V. CONCLUSION

The paper addresses the importance of network security using MAC address from the client. It also gives an overview of existing system which used IP address for blocking misbehaving users in anonymizing networks and its flaws in which honest users are blocked . This paper proposes a new improved method in which MAC address is used with a main motive of blocking only misbehaving users and giving full access rights to the honest users .

More over certificates are not used. Instead tickets generated from IP address are used. Sybil attack is also prevented. The users are well aware of the blacklisting status before accessing the server. The administrator can login from the client side and can delete the files or content present on server side .Tthe anonymous credentials systems are not used since tickets plays a vital role in the authentication Proposed system therefore overcomes the drawbacks present in existing system and its previous versions.

VI. REFERENCES

1. J.R. Douceur, “The Sybil Attack,” Proc. Int’l Workshop on Peer-to-Peer Systems (IPTPS), Springer, pp. 251-260, 2002.

2. P.P. Tsang, M.H. Au, A. Kapadia, and S.W. Smith, “Black-listable Anonymous Credentials: Blocking Misbehaving Users without TTPs,” Proc. 14th ACM Conf. Computer and Comm. Security (CCS ’07), pp. 72-81, 2007.

3. P.C. Johnson, A. Kapadia, P.P. Tsang, and S.W. Smith, “Nymble: Anonymous IP-Address Blocking,” Proc. Conf. Privacy Enhancing Technologies, Springer, pp. 113-133, 2007.

4. D. Boneh and H. Shacham, “Group Signatures with Verifier-Local Revocation,” Proc. ACM Conf. Computer and Comm. Security, 168-177, 2004.

5. R. Dingledine, N. Mathewson, and P. Syverson, “Tor: The Second-Generation Onion Router,” Proc. Usenix Security Symp., pp. 303-320, Aug. 2004.

6. D. Chaum, “Blind Signatures for Untraceable Payments,” Proc. Ann. Int’l Cryptology Conf. (CRYPTO), pp. 199-203, 1982.

7. D. Chaum and E. van Heyst, “Group Signatures,” Proc. Int’l Conf. Theory and Application of Cryptographic Techniques (EUROCRYPT), 257-265, 1991.

8. Lysyanskaya, R.L. Rivest, A. Sahai, and S. Wolf, “Pseudonym Systems,” Proc. Conf. Selected Areas in Cryptography, Springer,184-199, 1999.