Blocking Misbehaving Users In Anonymous Networks Using Nymble System

Senthil Kumar. B,
PG Student, Computer Science and Engineering,
Sree Sowdambika College of Engineering, Aruppukottai,
Tamil Nadu, India.

Saravanaselvam. N,
Professor, Computer Science and Engineering,
Sree Sowdambika College of engineering, Aruppukottai,
Tamil Nadu, India,

Abstract **- Anonymizing networks such as Tor allow users to access Internet services privately by using a series of routers to hide the client's IP address from the server. The success of such networks, however, has been limited by users employing this anonymity for abusive purposes such as defacing popular websites. Website administrators routinely rely on IP-address blocking for disabling access to misbehaving users, but blocking IP addresses is not practical if the abuser routes through an anonymizing network. As a result, administrators block all known exit nodes of anonymizing networks, denying anonymous access to misbehaving and behaving users alike. To address this problem, using present Nymble, a system in which servers can "blacklist" misbehaving users, thereby blocking users without compromising their anonymity. This system is thus agnostic to different servers' definitions of misbehavior servers can blacklist users for whatever reason, and the privacy of blacklisted users is maintained.**

Index Terms — Anonymous blacklisting, privacy, revocation.

I. INTRODUCTION

A. About the project

Anonymizing networks such as Crowds and Tor [6] route traffic through independent nodes in separate administrative domains to hide a client's IP address. Unfortunately, some users have misused such networks — under the cover of anonymity, users have repeatedly defaced popular websites such as Wikipedia. Since website administrators cannot blacklist individual malicious users' IP addresses, blacklist the entire anonymizing network. Such measures eliminate malicious activity through anonymizing networks at the cost of denying anonymous access to behaving users.

In other words, a few "bad apples" can spoil the fun for all. This has happened repeatedly with Tor. There are several solutions to this problem, each providing some degree of accountability. In pseudonymous credential systems [5], users are required to log into websites using pseudonyms, which can be added to a blacklist if a user misbehaves. Unfortunately, this approach results in pseudonymity for all

Anonymous credential systems [3] such as Camenisch and Lysyanskaya's systems use group signatures [1] for anonymous authentication Basic group signatures allow servers to revoke a misbehaving user's anonymity by complaining to a group manager. In these schemes, servers must query the group manager for every authentication, and this lack of scalability makes it unsuitable for future goals. Traceable signatures allow the group manager to release a trapdoor that allows all signatures generated by a particular user to be traced; such an approach does not provide the backward unlinkability that desire, where a user's accesses before the complaint remain anonymous.

B. Contributions Of This Project

- Blacklisting anonymous users. This project provides a means by which servers can blacklist users of an anonymizing network while maintaining their privacy.
- Practical performance. A system such as use widespread adoption only if its performance is acceptable at the server. This protocol makes use of inexpensive symmetric cryptographic operations to significantly outperform the alternatives.
- Open-source implementation. With the goal of contributing a workable system, this system built an open-source implementation of Nymble, which is publicly available and provide performance statistics to show that this system is indeed practical.

Some of the authors of this paper have published two anonymous authentication schemes, BLAC [12] and PEREA [13], which eliminate the need for a trusted third party for revoking users. While BLAC and PEREA provide better privacy by eliminating the TTP, Nymble provides authentication rates that are several orders of magnitude faster than BLAC and PEREA. Nymble thus represents a practical solution for blocking misbehaving users of anonymizing networks.

II. SYSTEM ANALYSYS

A. Existing System

The existing system does not provide much security and the anonymous users can change their IP address and come to the network may flood and spam the website.Wiki pedia site can't control this kind of misbehaving users.So the website get users IP address and block that misbehaving IP addresses.But anonymous users routing the IP address and use proxy server or some other IP changing software users can enter into network.

A1. Disadvantages

- This blocking system does not provide security ,any users can change IP and enter into network.
- There is no way to stop anonymity in this system and website admins can block only fake IP.

B. Proposed System

The present secure system called Nymble, which provides all the following properties:

- Anonymous authentication, backward unlinkability, subjective blacklisting, fast authentication speeds, rate limited anonymous connections, revocation auditability (where users can verify whether it have been blacklisted), and also addresses the Sybil attack [8] to make its deployment practical.
- In Nymble, users acquire an ordered collection of nymbles, a special type of pseudonym, to connect to websites. Without additional information, these nymbles are computationally hard to link, and hence using the stream of nymbles simulates anonymous access to services.
- Servers can therefore blacklist anonymous users without knowledge of their IP addresses while allowing behaving 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.
- 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 network(s) of choice.

B1. Advantages

- This new system find client mac or physical address and each time the client entry is maintained.
- When users misbehave in the website,admins can block their mac or physical address. so blocked user can't access internet services.
- This system works perfectly in LAN have to host this software and IIS server used to store information all the physical address and mac address.

C. Nymble System Architecture

Figure 2.1 shows the Nymble system architecture showing the various modes of interaction. Users interact with the PM directly, and with the NM and servers though the anonymizing network. All interactions not involving the user take place directly.

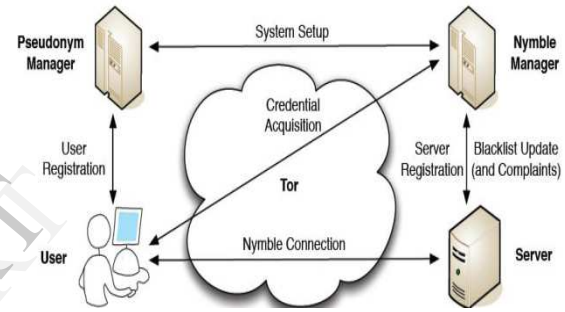

Fig. 1. Nymble System architecture

III. SYSTEM IMPLEMENTATION

A. Modules

A1. The Pseudonym Manager
A2. The Nymble Manager
A3. The Nymble Network
A4. Client Request/Response

A1. The Pseudonym Manager

The user must first contact the Pseudonym Manager (PM) and demonstrate control over a resource; for IP-address blocking, the user is required to connect to the PM directly (i.e., not through a known anonymizing network), assume the PM has knowledge about Tor routers, for example, and can ensure that users are communicating with it directly. Pseudonyms are deterministically chosen based on the controlled resource, ensuring that the same pseudonym is always issued for the same resource. Note that the user does not disclose what server user intends to connect to, and therefore the user's connections are anonymous to the PM.

The PM's duties are limited to mapping IP addresses (or other resources) to pseudonyms. As will explain, the user contacts the PM only once per likability window (e.g., once a day).

A2. The Nymble Manager

After obtaining a pseudonym from the PM, the user connects to the Nymble Manager (NM) through the anonymizing network, and requests nymbles for access to a particular server (such as Wikipedia). Nymbles are generated using the user's pseudonym and the server's identity.

The user's connections, therefore, are pseudonymous to the NM (as long as the PM and the NM do not collude) since the NM knows only the pseudonym-server pair, and the PM knows only the IP address-pseudonym pair. Note that due to the pseudonym assignment by the PM, nymbles are bound to the user's IP address and the server's identity.

To provide the requisite cryptographic protection and security properties (e.g., users should not to be able to fabricate their own nymbles), the NM encapsulates nymbles within nymble tickets. Servers wrap seeds into linking tokens and therefore will speak of linking tokens being used to link future nymble tickets. The importance of these constructs will become apparent as proceed.

A3. The Nymble Network

The Nymble Network is mainly used to connect the Nymble Manager, Pseudonym Manager and client. These three communicate with one another through on Nymble Network. The manger to validate the client through this network only. This network is formed in WCF concept. Through this network only the data will be stored in database.

A4. Client Request/Response

This module having two things one is net access and second one is mail access. Net access is mean that the client use the allowed website only. If the client use blocked website the client net access will be blocked using an MAC address (physical address). Mail Access: The client sends the mail to any the message will be stored in database. If the admin only to send the mail in particular id.

B. Server Registration

To participate in the Nymble system, a server with identity sid initiates a type-Auth channel to the NM, and registers with the NM according to the Server Registration protocol below. Each server may register at most once in any linkability window.

- The NM makes sure that the server has not already registered: If (sid; _; _) 2 nmEntries in its nmState, it terminates with failure; it proceeds otherwise.
- The NM reads the current time period and linkability window as t_{now} and w_{now}, respectively, and then obtains an svrState by running $NMRegisterServer_{nmState(}$sid; t_{now}; w_{now}).
- The NM appends svrState to its nmState, sends it to the Server, and terminates with success.
- The server, on receiving svrState, records it as its state, and terminates with success.

In svrState, macKeyNS is a key shared between the NM and the server for verifying the authenticity of nymble tickets; timelastUpd indicates the time period when the blacklist was last updated, which is initialized to tnow, the current time period at registration.

C. User Registration

A user with identity uid must register with the PM once in each linkability window. To do so, the user initiates a type- Basic channel to the PM, followed by the User Registration protocol described below.

- The PM checks if the user is allowed to register. In the current implementation, the PM infers the registering user's IP address from the communication channel, and makes sure that the IP address does not belong to a known Tor exit node. If this is not the case, the PM terminates with failure.
- Otherwise, the PM reads the current linkability window as w_{now}, andrunspnym:= PMCreatePseudonympmState(uid;wnow): The PM then gives pnym to the user, and terminates with success.
- The user, on receiving pnym, sets her state usrState to (pnym; ;), and terminates with success.

D. Nymble Connection Establishment

To establish a connection to a server sid, the user initiates a type-Anon channel to the server, followed by the Nymble connection establishment protocol described below.

D1. Blacklist Validation

- The server sends (blist; cert) to the user, where blist is its blacklist for the current time period and cert is the certificate on blist.
- The user reads the current time period and linkability window as t(U now) and w(U now) and assumes these values to be current for the rest of the protocol.

- For freshness and integrity, the user checks if VerifyBLusrState(sid; t(U now) ; w(U now); blist; cert)= true: If not, admin terminates the protocol with failure.

D2. Privacy Check

Since multiple connection establishment attempts by a user to the same server within the same time period can be linkable, the user keeps track of whether she has already disclosed a ticket to the server in the current time period by maintaining a boolean variable ticketDisclosed for the server in her state.

Furthermore, since a user who has been blacklisted by a server can have her connection establishment attempts linked to her past establishment, the user must make sure that she has not been blacklisted thus far.

Consequently, if ticketDisclosed in usrEntries[sid] in the user's usrState is true, or

UserCheckIfBlacklistedusrState(sid; blist) = true;

then it is unsafe for the user to proceed and the user sets safe to false and terminates the protocol with failure.

E. Service Provision and Access Logging

If both the user and the server terminate with success in the Nymble connection Establishment described above, the server may start serving the user over the same channel. The server records ticket and logs the access during the session for a potential complaint in the future.

IV. SCREEN SHOTS

Fig. 2. Server registration

Fig. 3. User login

Fig. 4. Mail usage, send mail

Fig 5. Mail Usage

Fig. 6. Net access details

V. CONCLUSION

In this comprehensive credential system called Nymble is built, which can be used to add a layer of accountability to any publicly known anonymizing network. Servers can blacklist misbehaving users while maintaining their privacy, and show how these properties can be attained in a way that is practical, efficient, and sensitive to needs of both users and services. This system provide how to get physical address and mac address of client system. Then admin can give permission or block access to particular web page each and every time must check whether the entered login id have access to this page or not. This system provide security to websites.

VI. FUTURE ENHANCEMENT

In future this system hosting to all sites and block the anonymous users by blocking their physical address and mac address instead of blocking their IP. Now this system works on LAN network. The future system will be configured for wireless, WAN, MAN networks and secure the website from anonymity.

REFERENCES

[1] Ateniese.G, J. Camenisch, M. Joye, and G. Tsudik, "A Practical and Provably Secure Coalition-Resistant Group Signature, Scheme," Proc. Ann. Int'l Cryptology Conf. (CRYPTO), Springer, pp. 255-270, 2000.

[2] Bresson.E and Stern.J, "Efficient Revocation in Group Signatures," Proc. Conf. Public Key Cryptography, Springer, pp. 190-206, (2001).

[3] Camenisch.J and Lysyanskaya.A, "An Efficient System for Non-Transferable Anonymous Credentials with Optional Anonymity Revocation," Proc. Int'l Conf. Theory and Application of Cryptographic Techniques (EUROCRYPT), Springer, pp. 93-118, (2001).

[4] Camenisch.J and Lysyanskaya.A, "Dynamic Accumulators and Application to Efficient Revocation of Anonymous Credentials," Proc. Ann. Int'l Cryptology Conf. (CRYPTO), Springer, pp. 61-76, (2002).

[5] Chaum.B, "Showing Credentials without Identification Transfeering Signatures between Unconditionally Unlinkable Pseudonyms," Proc. Int'l Conf. Cryptology (AUSCRYPT), Springer, pp. 246-264, 1990.

[6] Dingledine.R, N. Mathewson, and P. Syverson, "Tor: The Second- Generation Onion Router," Proc. Usenix Security Symp., pp. 303- 320, Aug. 2004.

[7] Damgard.I, "Payment Systems and Credential Mechanisms with Provable Security Against Abuse by Individuals," Proc. Ann. Int'l Cryptology Conf. (CRYPTO), Springer, pp. 328-335, (1988).

[8] Douceur .J.R, "The Sybil Attack," Proc. Int'l Workshop on Peer-to- Peer Systems (IPTPS), Springer, pp. 251-260, 2002.

[9] Johnson.P.C and Kapadia.A, P.P. Tsang, and S.W. Smith, "Nymble: Anonymous IP-Address Blocking," Proc. Conf. Privacy Enhancing Technologies, Springer, pp. 113-133, (2007).

[10] Lysyanskaya.A, Rivest.R.L, Sahai.A and Wolf.S, "Pseudonym Systems," Proc. Conf. Selected Areas in Cryptography, Springer, pp. 184-199, (1999). Micali.S, "NOVOMODO: Scalable Certificate Validation and Simplified PKI Management," Proc. First Ann. PKI

[11] Patrick P. Tsang, Apu Kapadia, Member, IEEE, Cory Cornelius, and Sean W. Smith"Nymble: Blocking Misbehaving Users in Anonymizing Networks" (2011).

[12] Tsang .P.P, M.H. Au, A. Kapadia, and S.W. Smith, "Blacklistable Anonymous Credentials: Blocking Misbehaving Users without TTPs," Proc. 14th ACM Conf. Computer and Comm. Security (CCS '07), pp. 72-81, 2007.

[13] Tsang .P.P, M.H. Au, A. Kapadia, and S.W. Smith, "PEREA: Towards Practical TTP-Free Revocation in Anonymous Authentication," Proc. ACM Conf. Computer and Comm. Security, pp. 333-344, 2008.

AUTHORS PROFILE

B. Senthil Kumar received his B.E degree in the area of Computer Science And Engineering from Anna University, India in 2010. Doing M.E in the area of Computer Science And Engineering.

Dr. N. Saravanaselvam is presently working as a Professor & Head of the Department of PG Department of Computer Science and Engineering at Sree Sowdambika College of Engineering, Aruppukottai, Tamilnadu, India. He has completed his B.E. Electronics and Communication Engineering and M.E. Computer Science and Engineering in Arulmigu Kalasalingam College of Engineering Krishnankoil, Srivilliputtur Under Madurai Kamaraj University, Madurai. Now he is completed his Ph.D. in Computer Science and Engineering at Anna University, Chennai. He has guided more than 40 B.E./M.E. Projects and 3 M.Phil Thesis. His field of interest is Network Engineering. He published 6 papers in International Journal. He is a Life Member of ISTE, IAEng and IACSIT.