An Efficient Restricting of bad Users among Unidentified Users in a Network

Shaik Shabana, M.Chandra Naik
M.Tech(CSE) Student, Assoc. Professor, Dept of CSE
St.Mary's Group of institution Guntur,AP,India

Abstract**:** In this paper, we develop a new system to enable service providers, such as website operators, on the Internet to restrict past abusive users of anonymizing networks (for example, Tor) from further causing trouble behavior, without compromising their security, and while maintain the security of all of the uncorrupt users. This system provides a security-preserving analogy of IP address banning, and is modeled after the well-known Nymble system.

Nymble is a system that provides a restricting mechanism to a server to protect it from unauthorized users connecting through anonymizing networks such as Tor. Anonymous networks allow anyone to visit the public locations of the network. With this users access the Internet services through a series of routers. , this hides the user's fact of remaining the same one and IP address from the server. This is the advantage for the disruptive behaviouring users to destroy popular websites. To avoid this, servers may try to block the bad user, but it is not possible in case of anonymous networks. In such categories, if the abuser routes through to carry out network, administrators restrict all known exit nodes of to carry out networks, denying anonymous access to disruptive misbehaving and behaving users. To conflict this problem, a nymble system is designed in which servers can Suspicion the bad users without compromising their quality. This paper explains the idea that the different service providers have different suspicioning policies. For example, Wikipedia might want to obstruction a user one day for the first disruptive misbehavior, one week for the second one, etc. In order to do this, we have to propose a dynamic link ability window whose length can be increased exponentially. Thus, at the start of each likability window, all service providers must reset their suspicions and forgive all prior disruptive misbehavior.

Keywords: Anonymous blacklisting, security, revocation, Pseudonymous systems, anonymous credential systems.

I. INTRODUCTION

Anonymity networks provide users with a means to communicate and share the information privately over the network. The Tor network is the largest deployed anonymity network; the main objective of this is to defend users against traffic analysis attacks by encrypting users' communications and routing them through a worldwide distributed network of volunteer-run relays. The capability to communicate without fear of network surveillance makes it possible for many number of users to express ideas or share knowledge that they might else not be agree to reveal for fear of persecution, punishment or simply embarrassment . On the other hand, some of the users use the mask of anonymity as a license to perform mischievous deeds such as trolling forums or cyber-vandalism. For this occurrence, some of the most popular websites (for example, Wikipedia and Slashdot) proactively ban any user connecting from a known anonymous communications network from sharing content, thus limiting freedom of expression..

The privacy and security offered by Tor is directly related to the size of its anonymity set; i.e., the number of users on the network. The fewer Tor users there are, the easier it is to figure out which one of them initiated a particular connection. As a result, if users are discouraged from using the system, the privacy and security of those who do continue to use it suffers in consequence. Similarly, the anonymity afforded to each user is related to the number of volunteers running Tor nodes. One of the side effect of Tor exit nodes being banned from popular web services is that the operators of these relays get banned from these services as well, because their connections come from the same IP address as their Tor relay. This state provides a fairly strong incentive for many would-be operators not to volunteer to run relays.

In this, a real need exists for systems that allow users to contribute content online, while preserving the capability of service providers to selectively ban individual users without compromising their anonymity. Not only would such a system benefit the estimated hundreds of thousands of existing Tor users, but it may also be a boon to wider acceptance of Tor. Indeed, the need for contributor suspicions processing has been acknowledged by few key people involved with the Tor Project. Thus, this is reasonable to expect that the operators of Tor might be willing to provide the infrastructure necessary to realize such a system, a situation that would greatly minimize the burden on service providers and lead to greater than adoption.

Several procedures have been proposed with the goal of allowing anonymous suspicioning of Tor users. The one of the original systems is to recreate the common practice of IP address banning, without actually revealing a user's IP address; so, these systems suffer from some security issues stemming from the use of trusted third parties (TTPs) who can easily illegal to violate a user's anonymity. The most popular of these is Nymble which is the system after which we model our own.

In this system credential systems users log into Web sites using pseudonyms, which can be added to a blacklist if a user misbehave does the activities. Suddenly, this procedure results in pseudonymity for all users, and weakens the anonymity provided by the anonymizing network. Anonymous credential systems provide group authentications. Basic group authentications allow servers to revoke bad user's anonymity by complaining to a group manager. Servers must questions the group manager for every authentication, and thus, lack of scalability. Findable authentications allow the group manager to release a trapdoor that provides all authentications generated by a particular user to be traced; this is an approach does not provide the backward unlink ability that we desire, where a user's accesses before the complaint remain anonymous. Backward unlink ability allows for what we call subjective blacklisting, where servers can blacklist users for whatever reason since the privacy of the blacklisted user is not at the risk. In this approaches without backward unlink ability need to pay careful attention to when and why a user must have all their connections linked, and users must worry about whether their behaviors will be judged fairly.

Subjective blacklisting is also better suited to servers like as Wikipedia, where bad users such as questionable edits to a Webpage, are hard to define in mathematical terms. In some of the systems, misbehavior can be defined precisely. For instance, double spending of an "e-coin" is considered misbehavior in cash systems following which the offending user is deanonymized. Suddenly, such systems work for only minimal definitions of misbehavior—it is very difficult to find more difficult notions of misbehavior onto "double spending" or related approaches.

II. PROBLEM STATEMENT

The network of the Tor is an overlay network; each union router (UR) runs as a normal user-level process without any special privileges. Each union router maintains a TLS connection to every other onion router. Each user runs local software called a union proxy to fetch directories, establish circuits across the network, and handle connections from user applications. These onion proxies accept TCP streams and multiplex them across the circuits. The union router on the other side of the circuit connects to the requested destinations and relays data. Each union router maintains a long-term identity key and a short-term union key. The identity key is used to sign TLS certificates, to sign the UR's router descriptor (a review of its keys, address, bandwidth, exit policy, and so on), and (by directory servers) to sign directories. The union key is used to decrypt requests from users to set up a circuit and negotiate ephemeral keys. The TLS protocol also establishes a short term link key when communicating between URs. Short-term keys are rotated and independently, to limit the impact of key compromise. In this way the Tor network forms between the user and a Web server. ANONYMIZING networks such as Tor 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 Web sites such as Wikipedia. Since Web site administrators cannot suspicion individual malicious users' IP addresses, they blacklist the entire anonymizing network. Such measures eliminate malicious activity through anonymizing networks at the cost of denying contributors access to behaving users. In other words, a few "bad apples" can spoil the fun for all. (This has happened repeatedly with Tor.1)

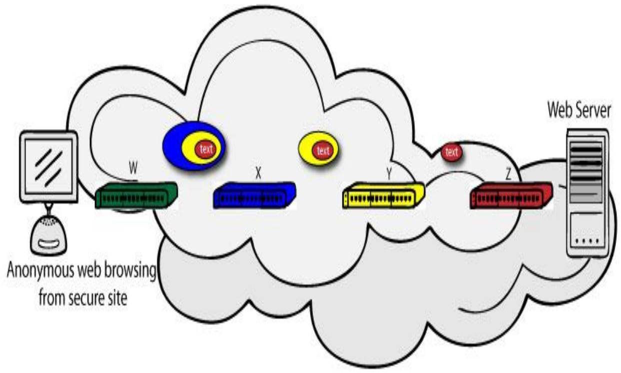


Fig1: Diagram of the Tor between web server and a user

III. PROPOSED SYSTEM NYMBLE OVERVIEW

In this we propose a secure based Nymble system; here users acquire an ordered collection of nymbles, a special type of procedure, to connect to Websites. Without additional information needed, these nymbles are computationally hard to link one to

another and hence, using the stream of nymbles simulates
contributors access to services. Web sites, however, can restrict users by gaining a seed for a particular nymble, allowing them to link future nymbles from the same user. Servers can therefore restrict anonymous users without knowledge of their IP addresses while allowing behaving users to connect anonymously. This system gives that users are aware of their restrict status before they present a nymble, and disconnect rapidly if they are restricted.

Hence this work applies to anonymizing networks in general, we consider Tor for purposes of statement. In fact, any number of anonymizing networks can rely on the same Nymble system, restricting anonymous users regardless of their anonymizing network(s) of choice. The purpose of the Nymble project is to allow for responsible, anonymous access online. It provides a mechanism for server administrators to obstruction misbehaving users while allowing for honest users to stay anonymous; in fact even the obstructioned users remain anonymous. The name "Nymble" comes from a play on the word "fictitious" and "nimble". Instead of giving users a simple fictitious, the Nymble system assigns users "nymbles"; that is, a fictitious with better anonymity properties.

3.1 Nymble properties:

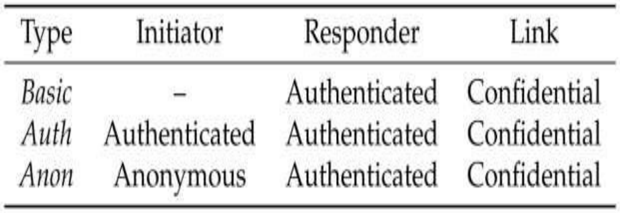
1. Restrict-status awareness: A user can check whether he/she has been obstructioned before accessing services at the server.

2. Anonymous blacklisting: A server can obstruction the IP address of a misbehaving user without knowing the identity of the user or his/her IP address.

3. Backward anonymity: The restricted user's previous activity remains anonymous/unlikable, and is refused future connections.

4. Subjective judging: Since misbehaving users are obstructioned without compromising their privacy, servers can provide their own definition of "misbehavior".

5. Privacy and security: Honest and misbehaving users both remain anonymous.



Type	Initiator	Responder	Link
Basic	–	Authenticated	Confidential
Auth	Authenticated	Authenticated	Confidential
Anon	Anonymous	Authenticated	Confidential

Fig. Different types of channels used in Nymble

3.2 Anonymizing Networks - Tor

Tor is an anonymizing network that hides a client's identity (actually, your computer's IP address) from the servers that it accesses. Tor keeps a client's IP-address anonymous by bouncing its data packets through a random path of relays. Each relay knows only of the relay that sent it data and the next relay in the random path. As long as the entry and exit nodes do not illegal, the client's connections remain anonymous. Tor provides anonymity, but some people abuse this anonymity. Since website administrators depend on obstructioning the IP addresses of misbehaving users, they are unable to obstruction misbehaving users who connect through Tor their IP address is hidden after all. Fulfilling a desired by repeated offenses through the Tor network, the usual response for websites such as Slashdot and Wikipedia is to an obstruction the entire Tor network. This is hardly an optimal solution, as honest users are denied anonymous access to these websites through Tor (or any anonymizing network for that matter).

3.3 Nymble for restricting Anonymous Users

To provide this mechanism for server administrators to an obstruction anonymous misbehaving users, we think to make the use of anonymizing networks like as Tor more acceptable for server administrators everywhere. In this all users remain anonymous— misbehaving users can be restricted without deanonymization, and their activity prior to being obstructioned remain unlinkable (anonymous).

In this we present a secure system called Nymble system, which provides all the following properties: authentication of anonymous, backward unlink ability, subjective restricting, very fast authentication speeds, rate-limited connections of anonymous, revocation audit ability, and also addresses the Sybil attack to make its deployment practical in Nymble, users can gain an ordered collection of nymbles, a special type of procedure, to connect to websites. Without additional information needed, these nymbles are computationally hard to link, and so using the stream of nymbles simulates anonymous access to services.

Websites, however, can restrict users by obtaining a seed for a particular nymble, allowing them to link future nymbles from the same user — those used before the complaint remains unlinkable. Servers can therefore restrict anonymous users without knowledge of their IP addresses while allowing behaving users to connect anonymously. Our system ensures that users are aware of their restrict status before they present a nymble, and disconnect immediately if they are restricted. Although our work applies to anonymizing networks in general, we consider Tor for purposes of statement. In fact, any number of anonymizing networks can rely on the same Nymble system, restricting anonymous users regardless of their anonymizing network(s) of choice

• **Restricting anonymous users**. We develop a means by which servers can restrict users of an anonymizing network while maintaining their privacy.

• **Practical performance**. This protocol provides the use of inexpensive symmetric cryptographic operations to significantly outperform the alternatives.

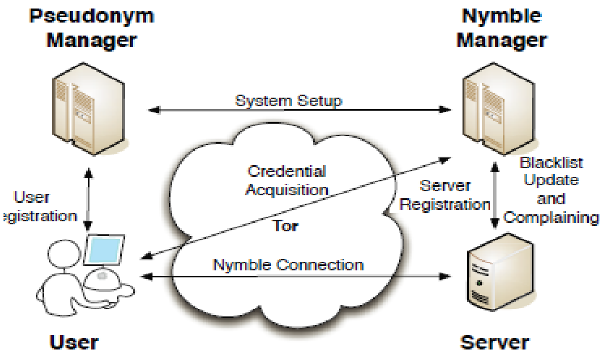


Fig2. The Nymble system architecture showing the various modes of interaction. Note that users interact with the NM and servers though the anonymizing network.

•**Implementation of the Open-source.** With this goal of contributing a workable system, we have construct an open source implementation of Nymble system, which is publicly available everywhere. We provide performance statistics to show that in this system is indeed practical.

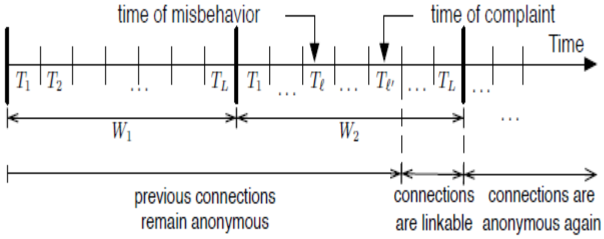
Nymble system is based on two administratively-separate "manager" servers, the fictitious Manager (PM) and the Nymble Manager (NM). The PM is used for pairing or connecting a user's IP address with a fictitious deterministically produced based on the user's IP address. The NM connects a user's fictitious with the target server. In some cases, long as the two managers are not colluding, the user's connections remain contributors to the PM, pseudonymous to the NM (note that the user does not communicate directly with the same NM, and connects to the NM through Tor), and contributors to servers that the user connects to.

3.4 Pseudonym Manager

The user (Alice) must first explained control over a resource that is the Alice's IP-address. To do this procedure Alice must first connect directly with the PM before receiving a fictitious. The PM has knowledge of existing Tor routers, and thus can give that Alice is communicating with it directly. Note that the PM has no knowledge of the user's destination, same case to the entry node in Tor. The PM sole is responsibility it to map IP addresses to pseudonyms.

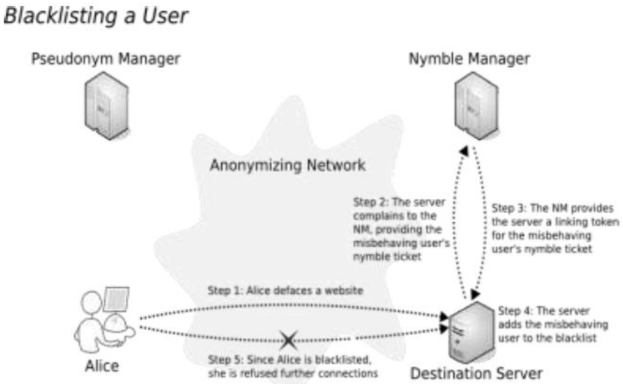
3.5 Nymble Manager

So Alice then connects to the NM through Tor presenting its pseudonym and her target server. The NM cannot know the IP address of the user, but the pseudonym provided by the PM guarantees that some unique IP address maps to their pseudonym Manager. She receives a set of nymble tickets as its credential for the target server. These nymble tickets are unlinkable, and so Alice can present these nymble tickets only once each to gain contributors access at the target server. The nymble ticket provides cryptographic secrete protection and security as well as a trap door that can be accessed using a linking token.



To provide the requisite cryptographic protection and security properties, the NM encapsulates nymbles within the nymble tickets, and trapdoors within linking tokens. So, we will explain the linking tokens being used to link future nymble tickets. The importance is illustrated in Figure 2, in this system, time is divided into likability windows of duration W, each of which is converted into smaller time periods of duration T , where the number of time periods in a likability window L = W/T is an integer. We called it as time periods and likability windows sequence of events as T1, T2, . . TL and W1, W2, . . respectively. Else a user's access within a time period is tied to a single nymble ticket, the use of different nymble tickets is a cross time periods permits the user anonymity between time periods—smallest time periods produce users with enough nymble tickets to operate contributors access. For example, T could is set to 5 minutes, and W is 1 day. The likability window serves two purposes—it allows for dynamism since IP addresses can get reconstructed to different well-behaved users, making it undesirable to restrict an IP address indefinitely, and it gives forgiveness of misbehavior after a certain period of time of these constructs will become apparent as we proceed.

3.6 Restricting a User


Blacklisting a User
Pseudonym Manager
Nymble Manager
Anonymizing Network
Step 2: The server complains to the NM, providing the misbehaving user's nymble ticket
Step 3: The NM provides the server a linking token for the misbehaving user's nymble ticket
Step 1: Alice defaces a website
Step 4: The server adds the misbehaving user to the blacklist
Alice
Step 5: Since Alice is blacklisted, she is refused further connections
Destination Server

Servers are used to present a user's nymble ticket to the NM as part of a complaint. The NM expands a "linking token" from the nymble ticket that is used to allow the server to link future connections by the restricted user. The NM also gives to servers with restricts, which users can tested before performing any actions at the server. By checking servers' restricts, restricted users are issued that their privacy and security is not compromised. Now we explain the process of restricting in a some more detail. In this we first explain how nymble tickets are bound to certain "time periods" and "likability windows."

This is done in two ways:

1. **Forgiveness:** It gives that bad behavior is forgiven after a certain period of time. Nymble is a system that allows websites to only selectively restrict users of anonymizing networks such as Tor without knowing the user's IP-address. Users not on the restrict enjoy anonymity while restricted users are not allowed future connections for duration of time while their previous connections remain unlinkable. Since Nymble allows websites to restrict anonymous users of their choice, and since users are notified of their restrict user status, Nymble gives websites the power to design their own definition of "misbehavior".
2. **Dynamism:** IP-addresses are reassigned to different users making it undesirable to permanently restrict IP-addresses.

3.7 Ticket Revocation

Ticket revocation is done, when a client is agreed and all his secrets are disclosed to the adversary. In this system adversary takes the ticket associated secrets from the compromised client and start retrieving the network services. When gateways contain records in the revocation database, they quickly report the revocation to the home TA, which will change and distribute and shared the revocation list for all gateways in the trust domain for reference.

IV. CONCLUSION

In this we present system that allows websites to only selectively obstruction users of anonymizing networks such as Tor. Using this system, websites can suspicion users without knowing their IP addresses. Users not on the suspicion enjoy anonymity, while blacklisted users are blocked from making future accesses. Furthermore, suspicion users' previous connections remain anonymous. So websites are free to suspicion anonymous users of their choice, and then users are notified of their blacklisting status, this system minimize the complications and difficulties associated with judging "misbehavior." We hope that these attributes will enhance the acceptability of anonymizing networks such as Tor by enabling websites to selectively block certain users instead of blocking the entire network, all else allowing the remaining users to stay anonymous.

References

[1] Johnson, P.C., Kapadia, A., Tsang, P.P., Smith, S.W.: Nymble: Anonymous IP-address blocking. In: Borisov, N., Golle, P. (eds.) Privacy Enhancing Technologies. Lecture Notes in Computer Science, vol. 4776, pp. 113{133. Springer (June 2007)

[2] B. Gedik and L. Liu, "Protecting location privacy with personalized k-anonymity: Architecture and algorithms," IEEE TMC,vol. 7, no. 1, pp. 1.18, 2008.

[3] Holt, J.E., Seamons, K.E.: Nym: Practical pseudonymity for anonymous networks. Internet Security Research Lab Technical Report 2006-4, Brigham Young University, Provo, UT, USA (June 2006)

[4] Brickell, E., Li, J.: Enhanced Privacy ID: A direct anonymous attestation scheme with enhanced revocation capabilities. In: Ning, P., Yu, T. (eds.) WPES. pp. 21{30. ACM (2007)

[5] Dingledine, R. harma@freehaven.neti: Re: Banned from Slashdot, http://archives.seul.org/or/talk/Jun-2005/msg00002.html, [Private e-mail message to Jamie McCarthy; 01-June-2005.

[6] J. Feigenbaum, A. Johnson, and P.F. Syverson, "A Model of Onion Routing with Provable Anonymity," Proc. Conf. Financial Cryptography, Springer, pp. 57-71, 2007.

[7] Lewman, A. handrew@torproject.orgi: Re: Talking w/local service CEOs [LJ, goog...], http://marc.info/?l=tor-talk&m=126137307104914&w=2, [Private e-mail message to hgrarpamp@gmail.comi; 21-December-2009]

[8] C. Cornelius, A. Kapadia, P.P. Tsang, and S.W. Smith, "Nymble: Blocking Misbehaving Users in Anonymizing Networks," Technical Report TR2008-637, Dartmouth College, Computer Science, Dec. 2008.

[9] CmdrTaco: Slashdot FAQ - accounts, http://slashdot.org/faq/accounts.shtml#ac900, [Online; accessed 11-January-2010; modified 02-July-2002]

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