Blocking of Mischievous Users in Anonymizing Networks using Nymble System

Srikanth Chintala, I.L. Narsimha Rao

Abstract— There are some networks called "Anonym zing networks" which allow users to gain access to internet services without revealing their identity (IP-addresses) to the servers. Networks such as "Tor (The Onion Router)","Crowds" and "I2P" gained popularity in the years 2002-2007, but the success of such networks however has been limited by users employing this anonymity for abusive purposes such as defacing popular websites such as "Wikipedia". Website Administrators blocks entire network which is connected to the abusive system to get rid of the abuser. Hence, well-behaved users also get blocked due to this action .To address this problem, we present a Nymble system in which servers can "blacklist" mischievous users without affecting good users and also maintaining anonymity across the network.

Index Terms- Anonymous, privacy, revocation, pseudonym, Blacklistability.

1 INTRODUCTION

Networks which provide anonymity to users such as Crowds and Tor [1], [2], will route the traffic through independent nodes in separate administrative domains to hide the user's IP address. Tor network routes through several series of routers to decrease the probability of predicting the IP address of the user by the server and hence increases the anonymity.

But unfortunately some users have misused such networks by taking the advantage of their anonymity to deface popular websites. Since website administrators cannot blacklist individual malicious users' IP addresses, they blacklist the entire anonymizing network. Such measures will definitely eliminate malicious activity through anonymizing networks, but at the same time it results in denial of service to behaving users as well. In other words, a poisonous fish can kill all other fishes under that same area. (This has happened repeatedly with Tor).

There are several solutions proposed to this problem so far, each providing some sort of accountability. "Pseudonymous credential systems" [4] was the first step towards the control of misbehaving users in anonymous networks. It was introduced by "Chaum" in 1985, as a way of allowing a user to work effectively and anonymously with multiple organizations. He suggested that each organization may know a user by a different pseudonym or simply a "nym". In pseudonymous credential systems, users log into websites using pseudonyms, which is added to the blacklist if a user misbehaves. Unfortunately, this method results in pseudonymity for all users and weakens the anonymity provided by the anonymizing networks.

"Anonymous Credential system" [5], [6] was introduced by Chaum and many anonymous credential systems have been proposed since then. Basically, this system employs group signatures [7], [8] which allow servers to revoke a misbehaving user's anonymity by complaining to a group manager.

Servers needs to query the group manager for every authentication and hence lacks scalability. Due to this reason, the anonymous credentials systems are least used now-a-days."Verifier-local revocation" [7] is another approach for our problem in which "Group signatures" are used. In this scheme, the server ("verifier") is required to perform only local updates during revocation. But unfortunately, VLR requires heavy computation at the server that is linear in the size of the blacklist properties.

2 OUR SOLUTION

We present a secure system called "Nymble" which provides the properties such as:

· Anonymous authentication
· Backward unlinkability
· Subjective blacklisting
· Fast authentication speeds
· Rate-limited anonymous connections
· Revocation auditability
· Anti-Sybil attack

In Nymble system [3], users acquire a collection of nymbles, a special type of pseudonym to connect to websites. Websites can blacklist users by obtaining a seed for a particular nymble, allowing them to link future nymbles from the same user by making the nymbles which were used before complaints remain unlinkable. Hence, servers can blacklist the anonymous users without knowledge of their IP addresses while allowing well-behaving users to connect anonymously. In this system, users should be aware of their blacklist status before they

Enter a nymble system and disconnect immediately if they are blacklisted.

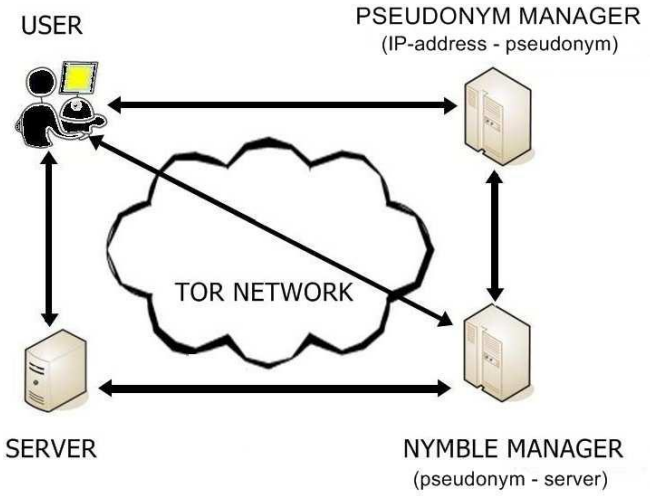


FIG.1 NYMBLE SYSTEM ARCHITECTURE

Above is the Nymble system architecture which has various modes of interaction in the network of anonymity. This system has overcome many drawbacks which arise from the previously proposed systems including the speed, computation work, security etc.

3 DEVELOPMENT TOWARDS APPROPRIATE SOLUTION:

The major need for creation of anonymizing networks is in the field of "Department of Defence (DoD)" in order to connect to server privately without revealing the user's identity. The first anonymous network was developed by Roger Dingledine, Nick Mathewson and Paul Syverson in September 2002 and it was named as "Tor (The onion Router)".

Tor is a system intended to enable online anonymity. Using Tor makes it difficult to trace internet activity, "including visits to websites, online posts, instant messages and other communication forms", and it is intended to protect users' personal freedom, privacy and ability to conduct confidential business by keeping their internet activities from being monitored. Above is the working of Tor network and encrypted nodes in that network.

A part from "Tor" there is many other anonymizing networks. Such as:

- Crowds
- I2P [12]
- Free net
- Phantom

3.1 Pseudonymous Credential Systems:

Pseudonymity technology is technology that allows individuals to reveal or prove information about themselves to others, without revealing their full identity.

A credential system is a system in which users can obtain credentials from organizations and demonstrate possession of these credentials. The idea of Pseudonymous credential systems was first put forwarded by "Anna Lysyanskaya", "R.L.Rivest" and "A.Sahai" in 1999 even before anonymous netwoks were developed.

In pseudonymous credential systems, users log into websites using pseudonyms. Pseudonyms are the false names used to hide users actual identities and maintains anonymity. Pseudonyms are generated by Tor client program itself and they are used to log into websites. Server maintains the blacklist of mischievous users by using pseudonyms provided by the users.

Advantages:

· Simple to implement
· Less computational

Drawbacks:

· It results in pseudonymity for all users
· Weakens the anonymity

3.2 Anonymous Credential Systems:

An anonymous credential system consists of users and organizations. Organizations know the users only by pseudonyms. The basic system comprises protocols for a user to join the system, register with an organization, obtain multi-show credentials, and show such credentials. Anonymous credential system was the innovation of "J.Camenisch" and "Anna Lysyanskaya" in the year 2001.They used the concept of "Group signatures" to make the system more efficient and anonymous.

Anonymous credential system consists of three parties i.e. users, an authority, and verifiers. These systems employ group signatures which allow servers to revoke a misbehaving user's anonymity by complaining to a group manager.

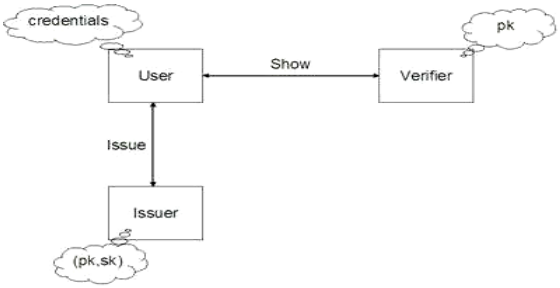


FIG.2 QUERYING TO GROUP MANAGER

Servers must query the group manager for every authentication and hence this system lacks scalability.

Advantages:

· Digital signatures ensure the security of system to some extent.

Drawbacks:

· Lacks scalability
· Backward unlinkability is not possible
· Servers can find users' IP addresses by using traceable Signatures

3.3 Verifier-Local Revocation (VLR):

In order to overcome the problem of lack of backward unlinkability VLR is proposed in 2004 by "Dan Boneh" and "Hovav Shacham".

An approach of membership revocation in group signatures is verifier-local revocation. In this approach, only verifiers are involved in the revocation mechanism, while signers have no involvement. Thus, since signers have no load, this approach is suitable for mobile environments. This scheme satisfies backward unlinkability to some extent. The backward unlinkability means that even after a member is revoked, signatures produced by the member before the revocation remains anonymous.

Verifier-local revocation requires the server ("verifier") to perform only local updates during revocation. Hence, there will be lot of burden on the server.

Advantages:

· Local updating is possible
· Backward unlinkability

Drawbacks:

· Heavy computational at server side
· Time consuming
· Less Secure

Hence, due to the unsatisfied results of the existing systems, we implemented the new Nymble system which can give us the fruitful results which we need.

4 Our Proposed Solution

Previously developed systems have so many drawbacks which restricted Tor and other anonymizing networks usage in the organizations. Hence, Nymble systems are proposed in order to overcome all those weaknesses and make the Tor a safe and efficient network.
In Nymble, users need to acquire an ordered collection of nymbles which is a special type of pseudonym in order to connect with websites. There is no restriction on the type of anonymizing network used i.e. it is not necessary that only Tor should be used here.

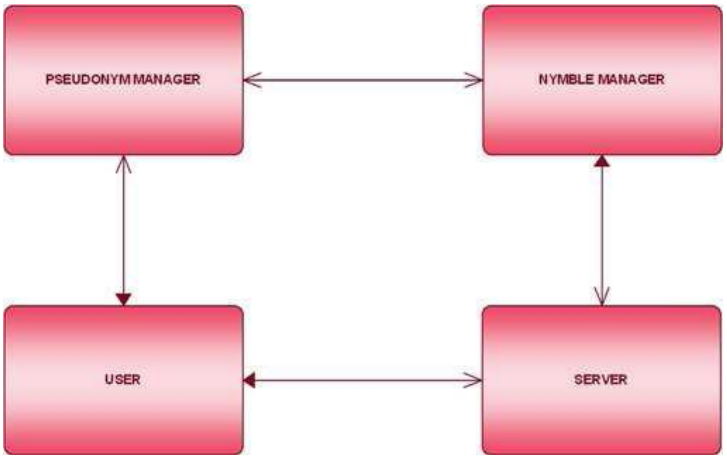


FIG.3 OVERVIEW SYSTEM DESIGN

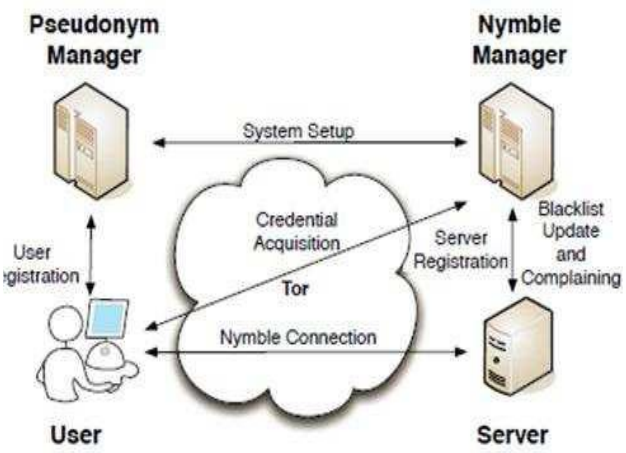


FIG.4 MODES OF NYMBLE SYSTEM

As we can see, Nymble system has various modes of interaction to different modules.

4.1 Working of Nymble:

Nymbles are generated by the "Nymble manager" based upon pseudonym and server ID. Websites can blacklist users by obtaining a seed for a particular nymble, allowing them to link future nymbles from the same user. One important thing which can be observed in our proposed system is that even though the future nymbles of the abusive user are linked, the nymbles that are used before complaint remain unlinkable. Hence, Nymble system guarantees backward unlinkability.

There are basically three modules in Nymble system. They are:

· Pseudonym Manager
· Nymble Manager
· Blacklisting a user

4.2 Pseudonym Manager

User need to contact the pseudonym manager and demonstrate control over a particular resource in order to get its IP-address blocked. The user is required to connect to the PM directly i.e. not through a known anonymizing network. Pseudonym Manager has the knowledge about Tor routers and hence it won't accept it if a user tries to connect with it with anonymizing network.

The basic idea behind connecting directly with Pseudonym Manager is that, it can identify the IP-address of the user. Pseudonyms are chosen based upon the controlled resource ensuring that the same pseudonym is always issued for the same resource. Pseudonym Manager only knows the IP address-pseudonym pair and hence it does not know the server to which the user wants to connect. User contacts the Pseudonym manager only once per linkability window (e.g. Once a day). The Pseudonym Manager issues pseudonyms to users. A pseudonym "pnym" has two components "nym" and "mac". "nym" is a pseudo-random mapping of the user's identity, the linkability window w for which the pseudonym is valid and PM's secret key nymKeyp. "mac" is a MAC that the Nymble Manager uses to verify the integrity of the pseudonym.

The below are the algorithms used in creation and verification of pseudonyms.

Algorithm `PMCreatePseudonym`
Input: $(uid, w) \in \mathcal{H} \times \mathbb{N}$
Persistent state: $pmState \in \mathcal{S}_P$
Output: $pnym \in \mathcal{P}$
1: Extract $nymKey_P, macKey_{NP}$ from $pmState$
2: $nym := \mathsf{MA.Mac}(uid||w, nymKey_P)$
3: $mac := \mathsf{MA.Mac}(nym||w, macKey_{NP})$
4: **return** $pnym := (nym, mac)$

Algorithm `NMVerifyPseudonym`
Input: $(pnym, w) \in \mathcal{P} \times \mathbb{N}$
Persistent state: $nmState \in \mathcal{S}_N$
Output: $b \in \{\text{true}, \text{false}\}$
1: Extract $macKey_{NP}$ from $nmState$
2: $(nym, mac) := pnym$
3: **return** $mac \stackrel{?}{=} \mathsf{MA.Mac}(nym||w, macKey_{NP})$

As we can clearly see, Pseudonyms are generated based upon user IP address i.e. uid, linkability window w and secret key.

4.3 Nymble Manager

After getting the pseudonym from the pseudonym manager, the user connects to the Nymble manager through anonymizing network and requests nymbles for access to a particular server.

Nymbles are generated using the user's pseudonym and the server's identity. Nymble Manager doesn't know anything about the user's identity. It knows only the pseudonym-server pair. Nymble Manager encapsulates nymbles within "Nymble tickets" in order to provide Cryptographic protection and security properties. Nymble Tickets are bound to specific time periods. In Nymble system, time is divided into linkability windows of duration W and each w is split into L time periods of duration T i.e. W=L*T.

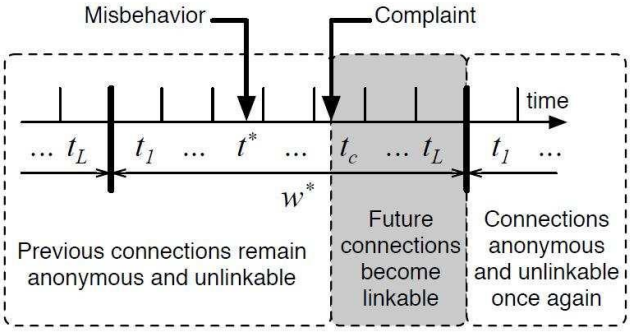


FIG.5 NYMBLE TICKETS ARE GENERATED

From the above fig, we can illustrate that future connections will become linkable for a particular current

window from which the complaint is registered and after that window the connections will be anonymous and unlinkable once again. This shows the backward unlinkable nature of our system.

Nymble Tickets are generated based upon the below algorithm

Algorithm NMCreateCredential

Input: $(pnym, sid, w) \in \mathcal{P} \times \mathcal{H} \times \mathbb{N}$

Persistent state: $nmState \in \mathcal{S}_N$

Output: $cred \in \mathcal{D}$

1: Extract $macKey_{NP}, macKey_N, seedKey_N, encKey_N$ from $keys$ in $nmState$
2: $seed_0 := f(\mathsf{Mac}(pnym||sid||w, seedKey_N))$
3: $nymble^* := g(seed_0)$
4: for t from 1 to L do
5: $seed_t := f(seed_{t-1})$
6: $nymble_t := g(seed_t)$
7: $ctxt_t := \mathsf{Enc.Encrypt}(nymble^*||seed_t, encKey_N)$
8: $ticket'_t := sid||t||w||nymble_t||ctxt_t$
9: $mac_{N,t} := \mathsf{MA.Mac}(ticket'_t, macKey_N)$
10: $mac_{NS,t} := \mathsf{MA.Mac}(ticket'_t||mac_{N,t}, macKey_{NS})$
11: $tickets[t] := (t, nymble_t, ctxt_t, mac_{N,t}, mac_{NS,t})$
12: end for
13: return $cred := (nymble^*, tickets)$

A credential contains all the Nymble tickets for a particular linkability window that a user can present to a particular Server. A ticket contains a nimble specific to a server, time period and linkability window.

4.4 Blacklisting a User

Whenever a user misbehaves, the server can link any future connection from that user within the current linkability window (e.g. the same day). Blacklistability assures that any honest server can indeed block mischievous users. Specifically, if an honest server complaint about a user that misbehaved in the current linkability window, the complaint will be successful and the user will be not able to nymble-connect to the server successfully in subsequent time periods.

Blacklisting can be implemented by using the below algorithm:

Algorithm UserCheckIfBlacklisted

Input: $(sid, blist) \in \mathcal{H} \times \mathcal{B}_n, n, \ell \in \mathbb{N}_0$

Persistent state: $usrState \in \mathcal{S}_U$

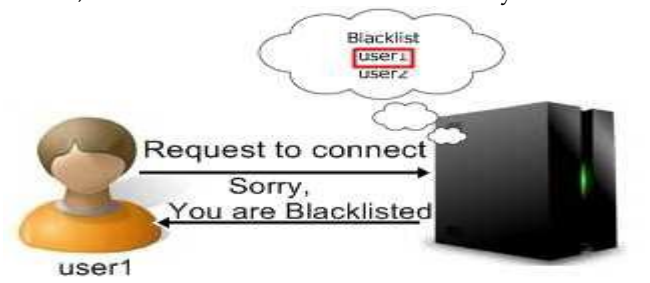
Output: $b \in \{\text{true}, \text{false}\}$

1: Extract $nymble^*$ from $cred$ in $usrEntries[sid]$ in $usrState$
2: **return** $(nymble^* \stackrel{?}{\in} blist)$

4.5 Notifying Users of Blacklist Status

Users who make use of anonymizing networks expect their connections to be anonymous. If a server obtains a seed for that user, it can link that user's subsequent connections. Users must be notified of their blacklisting status before they present a nymble ticket to a server.

In this system, the user can download the blacklist and verify whether he/she is on the blacklist. If he/she is on the list, then user can disconnect immediately.



In the above fig, we can see that user1is on the blacklist of the server. Hence, whenever user1 tries to access the server, there will be a "Denial of Service" to the user1.

User Registration:

User must first get registered with the pseudonym manager without using anonymizing networks.

Steps:-

· Pseudonym Manager checks if the user is allowed to register.
· Pseudonym manager makes sure that the connection is not from known Tor node.
· Pseudonym Manager reads the current linkability window.
· Pseudonym manager then gives "pnym" to the user.
· Pseudonym Manager terminates with success.
· The user sets his/her status on receiving pnym and terminates with success.

Server Registration:

Steps:-

· Server initiates a type-Auth channel to the Nymble Manager.
· Server registers with Nymble Manager.
· Nymble Manager makes sure that the server is not already Registered.
· If it's already registered, then Nymble Manager terminates with failure.

· If it's not registered then Nymble Manager reads the current time period and linkability window.
· Server on receiving its state by Nymble Manager records its state and terminates with success.

5 GOALS OF NYMBLE SYSTEM

Nymble aims for four security goals. They are:
· Blacklistability
· Rate-limiting
· Anonymity
· Non-frame ability

Blacklistability:

Blacklistability assures that any honest server can indeed block misbehaving users. Specifically, if an honest server complains about a user that misbehaved in the current linkability window, the complaint will be successful and the user will not be able to "nymble connect," i.e., establish a Nymble authenticated connection, to the server successfully in subsequent time periods (following the time of complaint) of that linkability window.

Rate-Limiting:

Rate-limiting assures any honest server that no users can successfully "nymbleconnect" to it more than once within any single time period.

Anonymity:

Anonymity protects the anonymous nature of honest users, regardless of their legitimacy according to the server.

Non-Frame Ability:

It guarantees that any honest user who is legitimate according to honest servers can nymble-connect to that server. This prevents an attacker from framing a legitimate honest user.

6 CONCLUSION

Efficient credential system called Nymble eliminated nearly all weaknesses and drawbacks in the previously developed systems to again make alive anonymizing networks which was blocked by many service providers. Servers can blacklist mischievous users while maintaining their privacy throughout the network. Even though there are still some issues related to backward unlinkability, this system provides enormous security properties.

Hope this new system will bring movement in the anonymizing networks usage and increase the mainstream acceptance of anonymizing networks such as Tor, Crowds,

I2P, etc. which has been completely blocked by several services because of users who abuse their anonymity.

7 ACKNOWLEDGEMENT

We would to thank the anonymous referee for helpful Comments.

8 REFERENCES

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

[2] www.torproject.org

[3] Patrick P. Tsang, Apu Kapadia, and Sean W.Smith, "Nymble: Blocking Misbehaving Users in Anonymizing Networks" IEEE March-April 2011.

[4] A. Lysyanskaya, R.L. Rivest, A. Sahai, and S. Wolf, "Pseudonym Systems," Proc. Conf. Selected Areas in Cryptography, Springer, pp. 184-199, 1999.

[5] J.Camenisch and A. Lysyanskaya, "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.

[6] 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.

[7] D. Boneh and H. Shacham, "Group Signatures with Verifier-Local Revocation," Proc. ACM Conf. Computer and Comm. Security, pp. 168-177, 2004.

[8] M. Bellare, H. Shi, and C. Zhang, "Foundations of Group Signatures: The Case of Dynamic Groups," Proc. Cryptographer's Track at RSA Conf. (CT-RSA), Springer, pp. 136-153, 2005.

Short Bio-Data for the Author

Mr. C. Srikanth received his B.Tech in Computer science and Engineering from Princeton Institute Of Technology And Sciences, JNTU, Hyderabad and Pursuing M.Tech in Computer science (Software Engineering) from Aurora's Technological And Research Institute, JNTU, Hyderabad.
Email: sreekanth.chintala@yahoo.com

Mr. I.L. Narsimha Rao working as Associate Professor in the Department of Computer Science and Engineering, in Aurora's Technological and Research Institute with a teaching experience of 15 years. He is also the chairman of CSI (**COMPUTER SOCIETY OF INDIA**), Hyderabad chapter 2012-2013.

Email: ilnrao@yahoo.com
chairman@csihyderabad.org