Nymble: Blocking Misbehaving Users In Anonymizing Networks

Prof. Vina Lomte[1], Pooja Gorlewar[2], Vishal Padghan[3],
Kritika Gunjegaonkar[4], Rashmi Kawale[5]
[12345]*(Padmabhooshan Vasantdada Patil Institute ofTechnology,Pune)*

Abstract: *The advent of anonymizing networks assured that users could access internet services with complete privacy avoiding any possible hindrance. This arrangement where series of routers form a network, hide the user's IP address from the server. However malfeasance of few malpractitioners has left this system with a loophole where users make use of this anonymity to deface popular websites. Administrators who cannot practically block a user using IP address are forced to shut all possible nodes that lead to exit. Thus deny access to both behaving and non-behavingusers altogether. And so end up blocking users with no compromise to their anonymity. Hence we propose a system which is undogmatic with different servers. Thus we aim at giving the administrator the right to block the malicious user without hindering the anonymity of the rest.*

Keywords: *anonym zing networks, blacklisting, symmetric cryptography, Tor, pseudonym, nymble ticket, Subnet-based blocking, Rate-limiting, Non-frame ability, Anonymous authentication, backward unlinkability, subjective blacklisting, rate-limited anonymous connections, revocation auditability.*

I. Introduction

We propose a system with following features: Anonymous authentication, backward unlink ability, subjective blacklisting, fast authentication speeds, rate-limited anonymous connections, revocation auditability (where users can verify whether they have been blacklisted). In this system we aim to generate nymbles, which are not easy to connect, however a stream of these nymbles assures we a simulation to anonymous access. Here we provide a means where the website administrator can block user without knowing his IP address (ie through pseudonym generated: which is a random secret identity with the pseudonym manager) without hindering the remaining network. User also has his complete privacy without having to compromise until he behaves.

II. Related Work

Anonymous credential systems like Camenisch and Lysyanskaya's [9, 10] use group signaturesfor anonymous authentication, wherein individual users are anonymous among agroup of registered users. Non-revocable group signatures such as Ring signatures [14]provide no accountability and thus do not satisfy our needs to protect servers from misbehaving users. Basic group signatures [3, 4, 2, 12] allow revocation of anonymity by no one except the group manager. As only the group manager can revoke a user's anonymity,servers have no way of linking signatures to previous ones and must query the group managerfor every signature; this lack of scalability makes it unsuitable for our goals.

Traceablesignatures allow the group manager to release a trapdoor that allows all signaturesgenerated by a particular user to be traced; such an approach does not provide thebackward anonymity that we desire, where a user's accesses before the complaint remainanonymous. Specifically, if the server is interested in blocking only future accesses of badusers, then such reduction of user anonymity is unnecessarily drastic.. And misbehavingusers should be blocked from making further connections after a complaint.

In some systems, misbehavior can be defined precisely. For instance, double-spendingof an "e-coin" is considered misbehavior in anonymous electronic cash systems [1,11]. Likewise, compact e-cash [6], k-times anonymous authentication [10] and periodic ntimesanonymous authentication [5] deem a user to be misbehaving if sheauthenticates"too many" times. In these cases, convincing evidence of misbehavior is easily collectedand fair judgment of misbehavior can be ensured. While such approaches can encouragecertain kinds of fair behavior in anonymizing.It is difficult to map more complex notionsof misbehavior onto "double spending" or related approaches. It may be difficult to preciselydefine what it means to "deface a webpage" and for Wikipedia to prove to a trustedparty that a particular webpage was defaced. How can the user be sure these "proofs" areaccurate and fairly judged? Can we avoid the problem of judging misbehavior entirely?In this paper we answer affirmatively by proposing a system that does not require proofof misbehavior. Websites may complain about users for any reason; our system ensuresusers are informed of complaints against them, thus "making everybody happy"—except,of course, the misbehaving users, who remain anonymous but are denied access.

Existing System

Verifier-Local Revocation (VLR): In order to overcome the problem of lack of backward unlinkability VLR was introduced in 2004 by "Dan Boneh" and "Hovav Shacham".This was an approach of membership revocation in group signatures known as verifier-local revocation. In this approach, only verifiers are involved in the revocation process, while there is no involvement of the signers. Thus, since signers have no load, this approach is suitable for mobile environments. This stratagem 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 to perform only local updates during revocation. Therefore, there will be a lot of burden on the server. Advantages of existing system are : 1)Local updating is possible 2)Backwardunlinkability

There are many solutions for the problems and difficulties in anonymous networks. But each method has some limitations and issues. They are like: In pseudonym Systems, every individual will be known to the other user by a pseudonym which is blacklisted if a user misbehaves. But this results in pseudonymity for all users and weakens the anonymity. And,also the users are prevented from sharing their pseudonyms.

Group signature is a method by which a member of a group anonymously signs the message on behalf of the group. Here, the server sends complaints to the Group Manager (GM) if a user misbehaves which lacks scalability. Traceable signatures traces the signatures signed by a single party without opening the signature and revealing the identities of any other users. It does not provide backward unlinkability, wherein the previously collected signatures remain anonymous even after the signer's revocation. Since there is no backward unlinkabilty, there will be no subjective blacklisting. Subjective blacklisting is the process by which the server can blacklist the user for whatever reason the server desires.

Drawbacks: ·
Heavy computation at the server side .
Time squander.
Less Secure

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

III. Proposed System

We present a 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 Without additional information, 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 seed for a particular nymble, allowing them to link future nymbles from the same user — those used before the complaint remainunlinkable. Servers can therefore blacklist anonymous users without knowledge of their IP addresses while allowing behaving users to connect anonymously. 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

Blacklisting anonymous users. We provide a means by which servers can blacklist users of an anonymizing network while maintaining their privacy.

Practical performance. Our protocol makes use of inexpensive symmetric cryptographic operations to significantly outperform the alternatives.

Open-source implementation. With the goal of contributing a workable system, Wehave built an open source implementation of Nymble, which is publicly available.I provide performance statistics to show that our system is indeed practical.

3.1 Advantages:

1. Intends to bind identity of an anonymous user to a pseudonym, generated from user's IP address. This idea enables a server to complainaboutmisbehavior of a user and blacklist his future tickets.
2. Honest users remain anonymous, &blacklist future connections of particular users and their requests remain unlinkable.
3. All connections of a blacklisted user before the complaint will remain anonymous.
4. A user can check whether he is blacklisted or not at the beginning of a connection.
5. Users are aware of their blacklist status before accessing a service.
6. Servers can blacklist users for whatever reason, and the privacy of blacklisted users ismaintained.

3.2 Mathematical model :

Pseudonym Creation

Equation:

$$\boxed{\begin{array}{l}\text{(a)}\quad f(x)=\sum_{i=0}^{i=n} U_i \\ \text{(b)}\quad Ps= P\,(f(x))\end{array}}$$

Where

- f(x) is function to concatenate all string of the field from the user profile
- Ui -> each profile attributes
- Ps-> Pseudonym
- P(f(x)) -> Random Function to calculate Pseudonym

Algorithm:

```
Input: Set U ={ u1,u2,u3……un}
Output: pseudonym (Ps)
Step 0: Get the User Profile attribute set U
Step 1: Convert all the attributes to String type
Step 2: Concatenate all the String to get a single String
Step 3: Get the auto incremented User ID as I
Step 4: x=ID mod 7
Step 5: for i=0 to String length
Step 6: Fetch xth character from the String
Step 7: Continue till 7 characters are selected
Step 8: concatenate all the 7 characters
Step 9: return Pseudonym
```

ATTACKS: A={A1,......An} is Attack Set

A1 Attack

Equation:

$$\boxed{f(\,A1\,) \Rightarrow UP_{data} > lim}$$

Where

- f(A1) is function to identify uploading excess amount of data attack
- UP_{data} -> Uploading data
- Lim -> Limits

Algorithm:

```
Input: User Uploading data UPdata, threshold size (lim)
Output: User Blocked State
Step 0: Get the User data on the web server
Step 1: Get the Current of the file size as $C_{lim}$
Step 2: if( $C_{lim}$> lim )
Step 3: Tag user as misbehavior user
Step 4: Get Pseudonym
Step 5: Add Pseudonym in blocked list
Step 6: Update User's state
Step 7: return user state
```

A2 Attack

Equation:

$$\boxed{f(\ A2\ ) \Rightarrow U_{data} \notin U_i}$$

Where

- f(A2) is function to identify DMA attack
- U_{data} -> Users Uploaded data
- U_i ->Respective User

Algorithm:

```
Input: User accessing data Udata
Output: User Blocked State
Step 0: Allow User to access data on the web server
Step 1: Get the user accessed data name as $U_{data}$
Step 2: if $U_{data}$ does not belongs to him
Step 3: Tag user as misbehavior user
Step 4: Get Pseudonym
Step 5: Add Pseudonym in blocked list
Step 6: Update User's state
Step 7: return user state
```

A4 Attack

Equation:

$$\boxed{f(\ A4\ )=>U_{pwd} \notin U_i}$$

Where

- f(A4) is function to identify Password attack
- U_{pwd} -> Users Password
- U_i ->Respective User

Algorithm:

Input: User password U_{pwd} and U_{name}

Output: User Blocked State

```
Step 0: Allow User to login in his account
Step 1: Get the user's credential like $U_{name}$ and $U_{pwd}$
Step 2: if $U_{pwd}$ does not belongs to $U_{name}$
Step 3: then warn user for 3 times
Step 4: Reset Password
Step 5: Mail New Password to Original user
Step 6: Get Pseudonym
Step 7: Add Pseudonym in blocked list
```

A5 Unblocking User

Equation:

$$\boxed{f(\ A5\ )=>(\ t_c - t_b\ )>T}$$

Where

- f(unb) is function to identify unblocking user
- t_c-> Current time
- t_b-> blocked time
- T-> threshold time

Algorithm:

Input: Blocked time as t_b, Current time as t_c and Threshold time as T

Output: Unblocked Blocked State

```
Step 0: Get tb and $t_c$ and T
Step 1: if $(t_c - t_b)$>T
Step 2: Get Pseudonym
Step 3: Add Pseudonym in unblocked list
Step 4: Update User's state
Step 5: return user state
```

IV. System Ovreview

4.1 Implemented Modules:

4.1.1. Nymble Manager:

Servers have the right to blacklist anonymous users without having to know their IP addresses while allowing behaving users to stay intact anonymously. The system ensures the user has complete knowledge about being blacklisted, that he should disconnect immediately if they are blacklisted. Although our work applies to anonym zing networks in general, we consider Tor for purposes of exposition. In fact, any number of anonym zing networks can rely on the same Nymble system, blacklisting anonymous users regardless of their anonym zing network(s) of choice.

4.1.2. Pseudonym Manager

The user must first contact the Pseudonym Manager (PM) and demonstrate control over a resource; for IP-address blocking, the user must connect to the PM directly (i.e., not through a known anonym zing network), ensuring that the same pseudonym is always issued for the same resource.

4.1.3. Blacklisting A User

Users who make use of anonym zing networks expect their connections to be anonymous. If a server obtains a seed for that user, however, it can link that user's subsequent connections. It is of utmost importance, then, that users be notified of their blacklist status before they present a nymble ticket to a server. In our system, the user can download the server's blacklist and verify her status. If blacklisted, the user disconnects immediately.

IP-address blocking employed by Internet services. There are, however, some inherent limitations to using IP addresses as the scarce resource. If a user can obtain multiple addresses she can circumvent both nymble-based and regular IP-address blocking. Subnet-based blocking alleviates this problem, and while it is possible to modify our system to support subnet-based blocking, new privacy challenges emerge; a more thorough description is left for future work.

4.1.4. Nymble-Authenticated Connection:

Blacklist ability 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 of that linkability window.Rate-limiting assures any honest server that no user can successfully nymble-connect to it more than once within any single time period. Non-frameability guarantees that any honest user who is legitimate according to an honest server can nymble-connect to that server. This prevents an attacker from framing a legitimate honest user, e.g., by getting the user blacklisted for someone else's misbehavior. This property assumes each user has a single unique identity.When IP addresses are used as the identity, it is possible for a user to "frame" an honest user who later obtains the same IP address. Non-frameability holds true only against attackers with different identities (IP addresses). A user is legitimate according to a server if she has not been blacklisted by the server, and has not exceeded the rate limit of establishing Nymble-connections. Honest servers must be able to differentiate between legitimate and illegitimate users.

Anonymity protects the anonymity of honest users, regardless of their legitimacy according to the (possibly corrupt) server; the server cannot learn any more information beyond whether the user behind (an attempt to make) a nymble-connection is legitimate or illegitimate

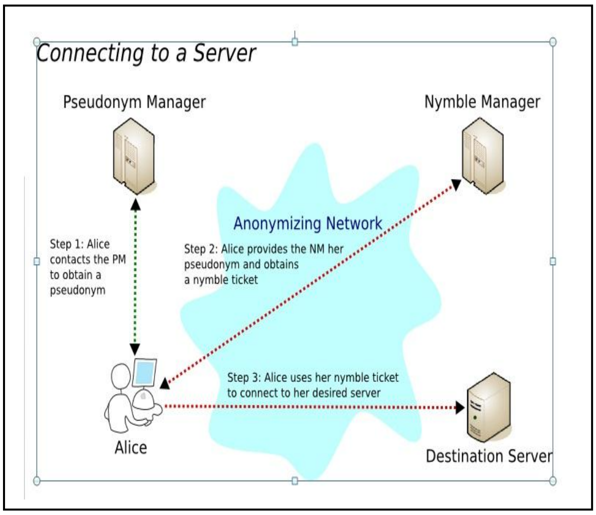
Connecting to a Server
Pseudonym Manager
Nymble Manager
Anonymizing Network
Step 1: Alice contacts the PM to obtain a pseudonym
Step 2: Alice provides the NM her pseudonym and obtains a nymble ticket
Step 3: Alice uses her nymble ticket to connect to her desired server
Alice
Destination Server

Fig.1 Pseudonym Manager

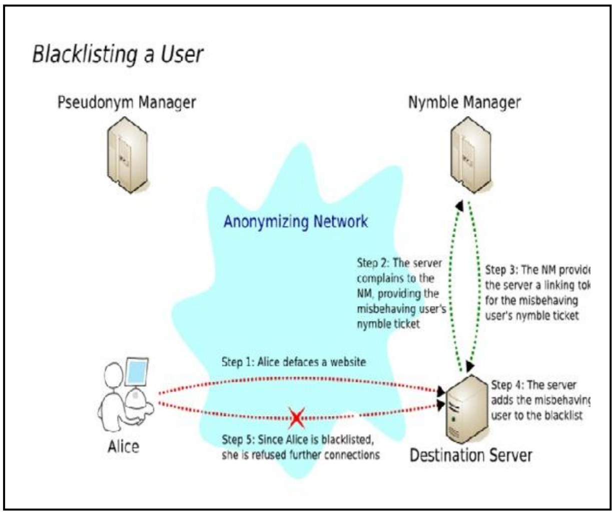
Blacklisting a User
Pseudonym Manager
Nymble Manager
Anonymizing Network
Step 2: The server complains to the NM, providing the misbehaving user's nymble ticket
Step 3: The NM provid the server a linking tok for the misbehaving user's nymble ticket
Step 1: Alice defaces a website
Step 4: The server adds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

Fig.2 Blacklist a User

V. Features

Anonymous Authentication: Anonymous authentication allows any user to access any public content without providing a user name and password challenge to the client browser. If some content should be viewed only by selected users, you must configure the appropriate permissions to prevent anonymous users from accessing that content. If you want only registered users to view selected content, configure an authentication method for that content that requires a user name and password.

Backward Unlinkability: Backward unlinkability means that even after a user is revoked, signatures produced by the user before the revocation remain anonymous. However, all the signatures produced from the revoked user are linkable. This means that the anonymity of signatures produced before the revocation is compromised. In some cases that all signatures from an illegal person should be traced. The approaches without backward unlinkability 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.

Fast Authentication Speed: In Nymble system there is a fast Authentication speed that implies the presence of a database to provide persistent data to be used as a part of the verification process. Database access must be kept to a minimum so that the request/response process remains fast and uninhibited by database overhead.

Revocation Auditability: In this the user can check whether he is blacklisted or not and if he is blacklisted then the user can be revoked

Subjective Blacklisting: if the authorized 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 a Nymble-authenticated connection.

Anonymity:A user is legitimate according to a server if user has not been blacklisted by the server, and has not exceeded the rate limit of establishing Nymble connections. Honest servers must be able to differentiate between legitimate and illegitimate users.
Non-frameability: It guarantees that any honest user who is legitimate according to an honest server can nymble connect to that server. This prevents an attacker from framing a legitimate honest user.
Rate limited anonymous connection: Rate-limiting assures any honest server that no user can successfully nymble-connect to it more than once within any single time period.

VI. Future Scope

Our nymble project can be extended in next version called nymble and also can be developed on android platform. We are expecting that our work will increase the mainstream acceptance of anonymizing networks such as Tor, which has thus far been completely blocked by several services because of users who abuse their anonymity. By providing a mechanism for server administrators to block anonymous misbehaving users, we hope to make the use of anonymizing networks such as Tor more acceptable for server administrators everywhere. All users remain anonymous misbehaving users can be blocked without deanonymization, and their activity prior to being blocked remain unlinkable

. This work can also be extended into a multiple rounds of pseudonym construction in which the PM participates in multiple rounds of communication with the user. Another enhancement would be is to provide service providers with the ability to detect repeat offenders and revoke these users' access for longer durations of time.

VII. Conclusion

We have proposed and built a comprehensive credentialsystem called Nymble, which can be used to add a layer ofaccountability to any publicly known anonymizing network.Our new design is not only scalable and robust, but also securer under various types of attacks.A new system is proposed that adds an additional layer of security to the anonymous networks.

In Our system we tried to blacklist user's activities,we have considered several types of attacks. This system is used to block the misbehaving users in anonymizing networks. It automatically finds the misbehaving user and blacklists them without affecting their privacy and anonymity. This adds one more layer of security to the system. The proposed method motivates the need for dynamic forgiveness and security in anonymous networks and this system will increase the acceptance of anonymous networks that is blocked by several services because of users who misuse their anonymity

Acknowledgments

We are greatly indebted to our college Padmabhooshan Vasantdada Patil Institute Of Technology that has provided a healthy environment to drive us to do this project and thankful to our management for their guidance

References

[1] Stefan Brands. Untraceable off-line cash in wallets with observers (extended abstract). In Douglas R. Stinson, editor, CRYPTO, volume 773 of LNCS, pages 302–318. Springer, 1993.
[2] Mihir Bellare, Haixia Shi, and Chong Zhang. Foundations of group signatures: The case ofdynamic groups. In Alfred Menezes, editor, CT-RSA, volume 3376 of LNCS, pages 136–153.Springer, 2005.
[3] Giuseppe Ateniese, Jan Camenisch, Marc Joye, and Gene Tsudik.A practical and provably secure coalition-resistant group signature scheme. In Mihir Bellare, editor, CRYPTO, volume1880 of LNCS, pages 255–270. Springer, 2000.
[4] Mihir Bellare, Daniele Micciancio, and Bogdan Warinschi. Foundations of group signatures: Formal definitions, simplified requirements, and a construction based on general assumptions.In Eli Biham, editor, EUROCRYPT, volume 2656 of LNCS, pages 614–629. Springer, 2003.
[5] Jan Camenisch, Susan Hohenberger, Markulf Kohlweiss, Anna Lysyanskaya, and MiraMeyerovich. How to win the clonewars: efficient periodic n-times anonymous authentication. InAri Juels, Rebecca N. Wright, and Sabrina De Capitani di Vimercati, editors, ACM Conferenceon Computer and Communications Security, pages 201–210. ACM, 2006.
[6] Jan Camenisch, Susan Hohenberger, and Anna Lysyanskaya.Compact e-cash. In RonaldCramer, editor, EUROCRYPT, volume 3494 of LNCS, pages 302–321. Springer, 2005.
[7] Paul F. Syverson, Stuart G. Stubblebine, and David M. Goldschlag.Unlinkable serial transactions.In Rafael Hirschfeld, editor, Financial Cryptography, volume 1318 of LNCS, pages39–56.Springer, 1997.
[8] Isamu Teranishi, Jun Furukawa, and Kazue Sako.k-times anonymous authentication. In Pil Joong Lee, editor, ASIACRYPT, volume 3329 of LNCS, pages 308–322.Springer, 2004.
[9] Jan Camenisch and Anna Lysyanskaya.An efficient system for non-transferable anonymous credentials with optional anonymity revocation. In Birgit Pfitzmann, editor, EUROCRYPT, volume2045 of LNCS, pages 93–118. Springer, 2001.
[10] David Chaum. Blind signatures for untraceable payments. In CRYPTO, pages 199–203, 1982.LNCS, pages 246–264. Springer, 1990.
[11] Patrick P. Tsang, Apu Kapadia, and Sean W. Smith.Anonymous IP-address blocking in torwith trusted computing (work-in-progress). In The Second Workshop on Advances in TrustedComputing (WATC '06 Fall), November 2006.
[12] Ronald L. Rivest, Adi Shamir, and Yael Tauman. How to leak a secret. In Colin Boyd, editor,ASIACRYPT, volume 2248 of LNCS, pages 552–565. Springer, 2001.