Privacy Preserving Technique for Blocking Misbehaviors in Anonymous Networks

Shatadal Patro[#], Asha Ambhaikar[*]

[#] 4th Sem MTech (SE), RCET, Bhilai, Sri Ram Colony, Rajnandgaon

[*]Prof. in Department of Computer Science & Engineering, RCET, Bhilai

Abstract

The facility of hiding the client's IP address from the server is provided by various anonymous networks similar to TOR and others. These networks provide a boon to users to access internet service privately by manipulating a series of routers to hide their IP address from the server. But this provision can be utilized both by the genuine users and misbehaving ones alike. The purpose of the facility provided by such kind of networks is being spoiled altogether by the miscreants. Due to this, the positive purpose of anonymous users. Because of this, the genuine accessibility of the behaving user's remains deterred. To surmount this problem, we present credential system, in which servers can blacklist misbehaving users. This system is unique because of its ability to disconnect the accessibility, all on a sudden, as soon as the misbehaving users have been blacklisted. As such, this system is a step forward towards attaining maximum efficiency.

Nymblewords: *Credential system, Revocation, Ticket Method, Anonymous blacklisting, Privacy.*

1. Introduction

There are so many anonymizing networks similar to TOR route traffic through independent nodes in separate administrative domains for hiding a client's IP address. In the name of anonymity some in genuine users resort to misuse of such networks, defacing popular websites such as Wikipedia. As website administrators are unable to blacklist individual malignant user's IP addresses, they blacklist the anonymizing network as a whole. As such, the anonymous access to behaving users is deterred because of the steps taken to eliminate the malicious activity of some users. Recurrences of such inconveniences have happened with Tor.

Variegated solutions are available for this problem which provides accountability to some extent pseudonymous credential system provides websites with pseudonyms which can be added to a blacklist in the case of a misbehaving user. But the very purpose of providing anonymity is weakened because of psedonymity for all users. Anonymous credential systems enable servers to complain a group manager by means of revoking a misbehaving user's anonymity. Lack of scalability occurs due to query of every authentication.

The desired 'Backward likability' is not provided as to where a user's accesses before the complaint remain anonymous. Subjective blacklisting is the advantage of backward likability, whereas the other approaches without backward likability need more concern about the 'when' and 'why' of the linked connection of the user. Subjective blacklisting is more advantageous to server like Wikipedia, where precise definitions are hard to make. Examples may be cited in cases like double spending of an "e-coin" which is considered as misbehavior. But it is not easy to map more complex notions of misbehavior. All the other existing user's credentials must be updated with dynamic accumulators and as such it is impractical.

1.1 Our Viable Solution

The secure system by name Security can provide the following facilities in one.

- Anonymous authentication,
- Backward unlinkability,
- Subjective blacklisting,
- Fast speed in authentication,
- Rate-limited anonymous connection,
- Revocation auditability,
- Capability to address Sybil attack.

As such, it enables the behaving users to connect anonymously, while servers can blacklist anonymous users without the knowledge or their IP addresses. In this system, the user-awareness and immediate disconnection are guaranteed about the blacklist status before they present a Security.

2. Outline of Security

In resource-based blocking to create a real-world deployment, some sort of resource-based blocking is a must.

2.1 Pseudonym & Security Manager

Direct contact of the user is mandatory towards the pseudonym manager for demonstrating control over a resource. Same pseudonyms are constantly issued for the same resource. The pseudonym manager's assignments are constrained to mapping IP addresses to pseudonyms. The user contacts the pseudonym manager only once per likability window.

The process starts with the connection to the Security manager, after obtaining a pseudonym by the user via anonymizing network. The user's requests to the Security manager are pseudonyms and nymble are specific to a particular user-server pair. The Security system cannot identify the specific user and the connected server. Until the pseudonym and Security manager do not collude. That shows the Security manager is familiar with only the pseudonym-server pair and the pseudonym manager deals only with the user identity-pseudonym pair.

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 we will speak of linking tokens being used to link future nymble tickets. The importance of these constructs will become apparent as we proceed.

2.2 Blacklisting a User & Blacklisting Status

In case a user misbehaves; any future connection may be linked by the server within the current linkability window. The provision of backward linkability and subjective blacklisting are facilitated, because the user's past connections remain unlinkable inspite of the future blocking of the misbehaving user.

In the present system, the facility of notification of the blacklist status is possible, by downloading the server's blacklist; a user can verify the status and immediately disconnect it. The authenticity of the blacklist can easily be verified, provided that the list is updated in the current time period. If it is not updated as such, the "daisies" provided by Security manager ensures the updated version. We can be sure about the non existence of race conditions in the verification of freshness of a blacklist, due to the use of 'digital signatures' and 'daisies'.

In the updates to the Security protocol the privacy properties associated with nymble alone had already been proved as part of a two-tiered hash chain. Now the security at the protocol level is to be proved. It is a process of redesigning and refining the definitions of the protocols to protect against towards privacy. As such a large anonymity sets are created by preventing the server from distinguishing between the users already connected in the same time period and those who are blacklisted. By this process, servers obtain proofs of freshness every time period for easy download verification. To assure efficiency of the blacklist updating, lightweight daisies are issued by NM to servers as proof of freshness. The NM embeds a distinct identifier Security for direct recognition. Time is divided into linkability windows of duration W, each of which is split into L time periods of duration T (i.e., W=L*T).

3. Security Goals

Four security goals are to be achieved. They are blacklistability, Rate limiting, Non-frameability, anonymity. In Blacklistability it gives assurance of blocking misbehaving users,

thereby preventing the misbehaving user disabling him from establishing a Security authentication connection to the server successfully in the forthcoming time periods. Rate-limiting is a preventive technique, which assures any honest server that no user can successfully connect to Security more than once within any single time period.

Nonframeability assures the genuine user who is legitimate as per the honest server can Security- connect to that server. By this, the genuine user is protected from being framed, and erroneously blacklisted for someone else's misbehavior. It is to be noted that, nonframeability against attackers with different identities. It is mandatory that servers are able to differentiate between valid and invalid users. In anonymity genuine users is protected notwithstanding their legitimacy status as per the server. The server's assignment is mainly concerned only with learning the legitimacy or otherwise of the user behind a Security connection. Fig (1) shows the activity of the credential system.

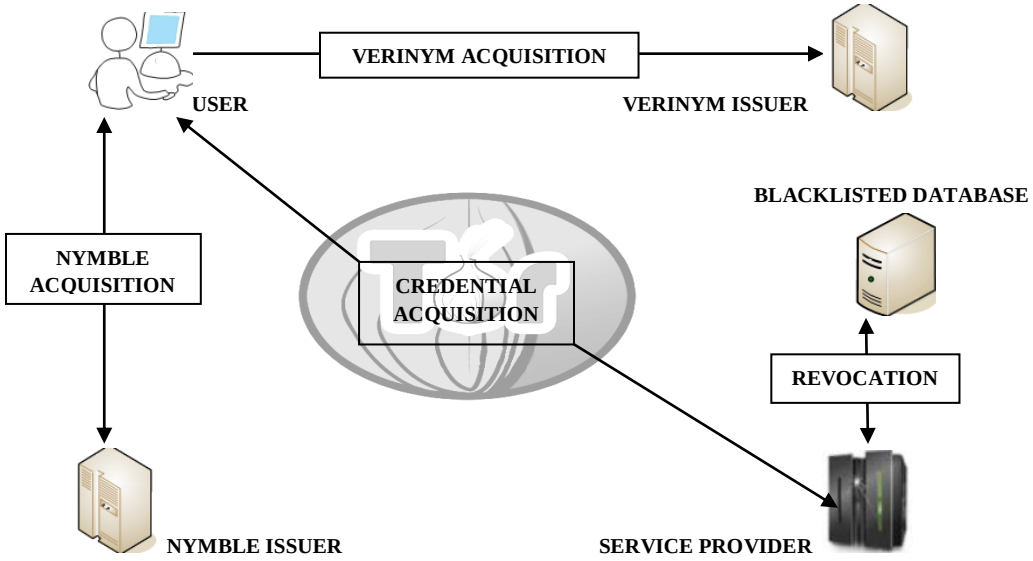

Fig.1-Credential System Architecture

3.1 Modifying Blacklist

Server updates their blacklists for two purposes.

- Server needs to provide the user with its blacklist
- For processing the newly filed complaints.

The procedure of updating blacklists differs on the involvement of complaints. In case of no complaints blacklist remains unchanged. If there are complaints new entries are added to the blacklists and the certificates are to be regenerated. So multiple updates within a single time period are not allowed. In present implementation the server updates its blacklist upon its first credential connection establishment request in a time period. Without Complaints and With Complaints these ways Updating of blacklist taken place.

4. Procedure

4.1 Pseudonyms

The PM issues pseudonyms to users. A pseudonym pnym has components nym and mac: nym is a pseudorandom mapping of the user's identity (e.g., IP address), the likability window w for which the Pseudonym is valid, and the PM's secret nymble nymNymbleP; mac is a MAC that the NM uses to verify the integrity of the pseudonym. Algorithms 1 and 2 describe the functions of creating and verifying pseudonyms.

4.2 Blacklist

A server's blacklist is a list of nymble*s corresponding to all the nymbles that the server has complained about. Users can quickly check their blacklisting status at a server by checking to see whether their nimble* appears in the server's blacklist (see Algorithm 3).

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

Algorithm 2. NMVerifyPseudonym
Input: $(pnym, w) \in \mathrm{P} \times \mathrm{N}$
Persistent State: $nmState \in S_N$
Output: $b \in \{true, false\}$
1: Extract $macKey_{NP}$ from $nmState$
2: $(nym, mac) := pnym$
3: **return** $mac \stackrel{?}{=} \mathrm{MA.Mac}(nym||w, macKey_{NP})$

Algorithm 3. UserCheckIfBlacklisted
Input: $(sid, blist) \in \mathrm{H} \times \mathrm{B}_n, n, l \in \mathrm{N}_0$
Persistent State: $userState \in S_U$
Output: $b \in \{true, false\}$
1:Extract $nymble^*$ from $cred$ in $usrEntries[sid]$ in $userState$
2:**return** $\left(nymble^* \stackrel{?}{\in} blist\right)$

Blacklist integrity. It is important for users to be able to check the integrity and freshness of blacklists, because, otherwise, servers could omit entries or present older blacklists and link users without their knowledge.

4.3 Server registration

A Server with identity *sid* initiates a type-Auth channel to the nymble manager for participation in the nymble system. It gets registered with the nimble manager as per the server registration protocol. Each server can register to a maximum of once in any linkability window.

Algorithm 4. NMRegisterServer
Input: $(sid, t, w) \in \mathrm{H} \times \mathrm{N}^2$
Persistent State: $nmState \in S_N$
Output: $srvState \in S_S$
1: $(keys, nmEntries) := nmState$
2: $macKeys_{NS} := \mathrm{Mac.KeyGen}()$
3: $daisy_L \in_R \mathrm{H}$
4: $nmEntries' := nmEntries \parallel (sid, macKeys_{NS}, daisy_L, t)$
5: $nmState := (keys, nmEntries')$
6: $target := h^{(L-t+1)}(daisy_L)$
7: $blist := \theta$
8: $cent := \mathrm{NMSignBL}_{nmState}(sid, t, w, target, blist)$
9: $srvState := (sid, macKey_{NS}, blist, cert, \theta, \theta, \theta, t)$
10: **return** $srvState$

In svrState, macNymbleNS is shared between the NM and the server for verifying the genuineness of nymble tickets; timelastUpd shows the time period when the blacklist was last updated, which is formatted to tnow, the current time period at registration.

Nymble utilizes three types of communication channels, namely, type-Basic, -Auth, and -Anon. We assume that a public-nymble infrastructure (PKI) such as X.509 is in place, and that the NM, the PM, and all the servers in Nymble have obtained a PKI credential from a well established and trustworthy CA. All users can realize type-Basic channels to the NM, the PM, and any server, again by setting up a TLS connection. Additionally, by setting up a TLS connection over the Tor anonymizing network, users can realize a type-Anon channel to the NM and any server.

5. Results & Screenshots

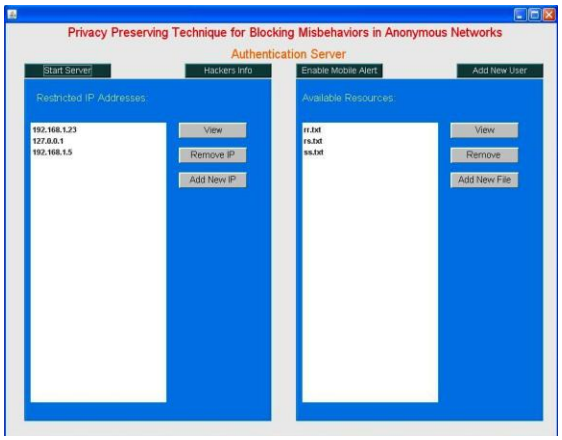

Fig.2-Authentication Server

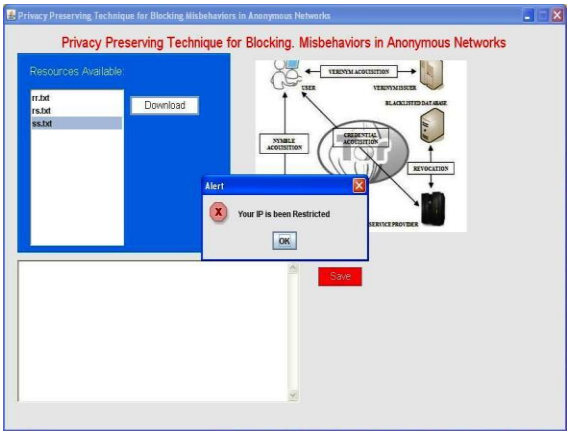

Fig.3-Client Window

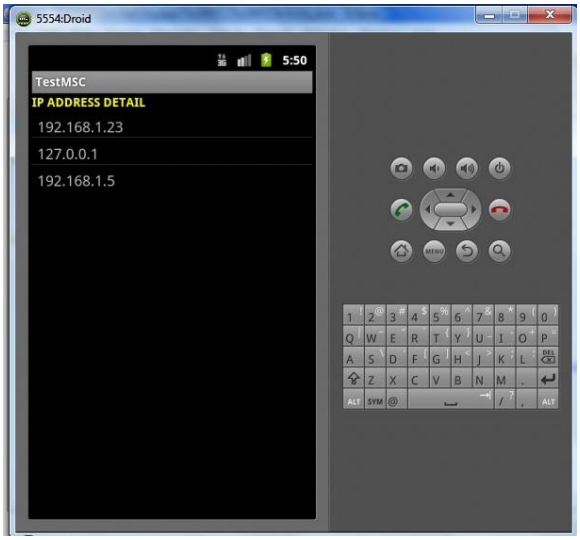

Fig.4-Mobile Alert on Android

6. Conclusion

We have proposed and built a comprehensive credential system called Nymble, 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 we show how these properties can be attained in a way that is practical, efficient, and sensitive to needs of both users and services.

We hope 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.

References

[1] Patrick P.Tsang, Apu Kapadia, Cory Cornelius, Sean W.Smith, "Nymble: Blocking Misbehaving Users in Anonymizing Networks", IEEE Transaction on Dependable and Secure Computing, Vol-8, No.2, March-April 2011

[2] Reed S. Abbott, TimothyW. van der Horst, and Kent E. Seamons. CPG: Closed Pseudony-mous Groups. In Vijay Atluri and Marianne Winslett, editors, Proceedings of WPES 2008, pages 55–64. Association for Computing Machinery (ACM) Press, New York, NY, USA, October 2008. (One citation on page 17.)

[3] Peter C. Johnson, Apu Kapadia, Patrick P. Tsang, and Sean W. Smith. Nymble:Anonymous IP-Address Blocking. In Privacy Enhancing Technologies, LNCS 4776, pages 113–133. Springer, 2007.

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

[5] Tadayoshi Kohno, Andre Broido, and K. C. Claffy. Remote physical device finger-printing. In Proceedings of the 2005 IEEE Symposium on Security and Privacy, pages 211–225, Washington, DC, USA, 2005. IEEE Computer Society.

[6] Toru Nakanishi and Nobuo Funabiki. Verifier-Local Revocation Group Signature Schemes with Backward Unlinkability from Bilinear Maps. In ASIACRYPT, LNCS3788, pages 533–548. Springer, 2005.

[7] Mihir Bellare, Haixia Shi, and Chong Zhang. Foundations of Group Signatures: TheCase of Dynamic Groups. In CT-RSA, LNCS 3376, pages 136–153. Springer, 2005.

[8] Dan Boneh and Hovav Shacham. Group Signatures with Verifier-Local Revocation. In ACM Conference on Computer and Communications Security, pages 168–177. ACM, 2004.

[9] RogerDingledine, Nick Mathewson, Paul Syverson,"Tor: The Second-Generation Onion Router," Proc.Usenix Security Symposium, pp. 303-320, 2004.

[10] A. Kiayias, Y. Tsiounis, and M. Yung, "Traceable Signatures," Proc. Int'l Conf. Theory and Application of Cryptographic Techniques (EUROCRYPT), Springer, pp. 571-589, 2004.

[11] Jan Camenisch and Anna Lysyanskaya. Signature Schemes and Anonymous Credentials from Bilinear Maps. In CRYPTO, LNCS 3152, pages 56–72. Springer, 2004.

[12] I. Teranishi, J. Furukawa, and K. Sako, "k-Times Anonymous Authentication (Extended Abstract)," Proc. Int'l Conf. Theory and Application of Cryptology and Information Security (ASIACRYPT), Springer, pp. 308-322, 2004.

[13] Giuseppe Ateniese, Dawn Xiaodong Song, and Gene Tsudik. Quasi-Efficient Revo-cation in Group Signatures. In Financial Cryptography, LNCS 2357, pages 183–197.Springer, 2002.

[14] Jan Camenisch and Anna Lysyanskaya. An Efficient System for Non-transferable Anonymous Credentials with Optional Anonymity Revocation. In EUROCRYPT,LNCS 2045, pages 93–118. Springer, 2001.

[15] Emmanuel Bresson and Jacques Stern. Efficient Revocation in Group Signatures. In Public Key Cryptography, LNCS 1992, pages 190–206. Springer, 2001.

[16] U.R.V.Nandhiny, M.B.Bose, R.Swathiramya, P.Elakiyaselvi , K.Lavanya, P.Yatheesha," A Ticket Based Method for Obstructing Abuser in Anonymous Network", IJCSNS International Journal of Computer Science and Network Security, VOL.12 No.1, January 2012