A Ticket Based Method for Obstructing Abuser in Anonymous Network

U.R.V.Nandhiny[†] , M.B.Bose[††], R.Swathiramya[†††],P.Elakiyaselvi[††††] ,K.Lavanya[†††††],P.Yatheesha[††††††]

PG Student ,Periyar Maniammai University,Thanjavur,TamilNadu,India
[††]Department of information technology,Periyar Maniammai University,Thanjavur,Tamil Nadu,India
[†, †††††] Department of Computer Science and Engineering,PPG Insitute Of Technology,Coimbatore,India

Summary
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 efficacy.

Key words:
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 *Nymble* 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 nymble.

Manuscript received January 5, 2012
Manuscript revised January 20, 2012

2.Outline Of Nymble

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

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

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 nymble 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 nymble protocol the privacy properties associated with nymbles 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 nymble 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 nymble 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 nymble more than once within any single time period. Nonframeability assures the genuine user who is legitimate as per the honest server can nymble- 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 nymble connection. Fig (1) shows the activity of the credential system.

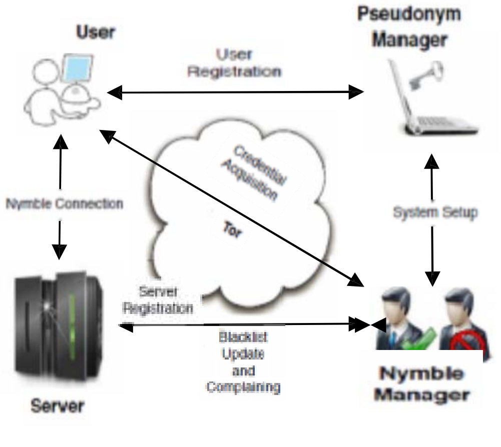

Figure 1: Credential System Architecture

3.1Modifying 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 nymble 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 key nymKeyP ; 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.

```
Algorithm 1. PMCreatePseudonym
Input: $(uid, w) \in \mathrm{H} \text{ x } \mathrm{N}$
Persistent State: $pmState \in S_P$
Output: $pnym \in \mathrm{P}$
Extract $nymKey_{P}, macKey_{NP}$ from $pmState$
$nym := \mathrm{MA.Mac}(uid||w, nymKey_{P})$
$mac := \mathrm{MA.Mac}(nym||w, macKey_{NP})$
return $pnym := (nym, mac)$
```

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

4.2.Blacklists

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

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: $(sid, t, w) \in \mathrm{H} \text{ x } \mathrm{N}^2$
Persistent State: $nmState \in S_N$
Output: $srvState \in S_S$
$(keys, nmEntries) := nmState$
$macKeys_{NS} := \mathrm{Mac.KeyGen}()$
$daisy_L \in_R \mathrm{H}$
$nmEntries' := nmEntries \,||\, (sid, macKeys_{NS}, daisy_L, t)$
$nmState := (keys, nmEntries')$
$t\arg et := h^{(L-t+1)}(daisy_L)$
$blist := \theta$
$cent := \mathrm{NMSignBL}_{nmState}(sid, t, w, t\arg et, blist)$
$svrState := (sid, macKey_{NS}, blist, cert, \theta, \theta, \theta, t)$
return $srvState$
```

In svrState, macKeyNS 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-key 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.Security Analysis

In Blacklistability because of the security of HMAC only the NM can issue valid tickets and can thus make mostly c connections to the server in any time period regardless of the server's blacklisting. The coalition cannot authenticate in the current time period k if each of the c users has been blacklisted in some previous time period of the current likability window. If we assure the contrary ,the connection establishment k using one of the coalition members ticket was successful even though the user was blacklisted in a previous time period k'.Because the connection establishments k' and k* were successful, the corresponding tickets ticket' and ticket* must be valid. In Non-frameability because of the security of HMAC, and since the PM and NM are honest, the adversary cannot force tickets for user i* and the server cannot already have seen ticket*.Thus there exists an entry in the server's linking list, such that the nymble in ticket* equals nymble*.In anonymity there are two anonymity sets of legitimate and illegitimate users. Every illegitimate user will evaluate 'safe' to false. so they terminate the protocol with failure at the end of the privacy check stage. An illegitimate user who has not disclosed a ticket during the same time period must already be blacklisted since an honest NM never deletes entries from a blacklist, it will appear in all subsequent blacklists and 'safe' is evaluated to false for the current blacklist. Server cannot forge blacklists or present blacklists for earlier time periods. This is the difference between two illegitimate users. Distinguishing between two legitimate users. The authenticity of the channel implies that a legitimate user knows the correct identity of the server and as

Such, Boolean ticket disclosed for the server remains false. Now, in the ticket presented by the user, only nymble and ctxt are functions of the user's identity. Since the adversary does not know the decryption implies that ctxt reveals no information about the user's identity to the adversary. Finally since the server has not obtained any seeds for the user, under the random oracle model, the nymble presented by the user is indistinguishable from random and cannot be linked with other nymbles presented by the user. When the server complains about a user's tickets in the future, the NM ensures that only one real seed is issued and thus the server cannot distinguish between legitimate users for a particular time period by issuing complaints in a future time period. In across multiple linkability windows our nymble construction has accountability and nonframeability because each ticket is valid for and only for a specific linkability window. It has 'Anonymity' because pseudonyms are an output of a collision-resistant function that takes the linkability window as input. Fig (2) shows the performance of normal users in x-axis shows the number of entries in each data structure's-axis for time duration of entries of normal users. There is no connection termination because of normal behavior of user. Fig (3) clearly shows the disconnection activity. If the user is blacklisted because of doing misbehaving activity as soon as the NM disconnects the process of that particular user. It does not interrupt other normal users.

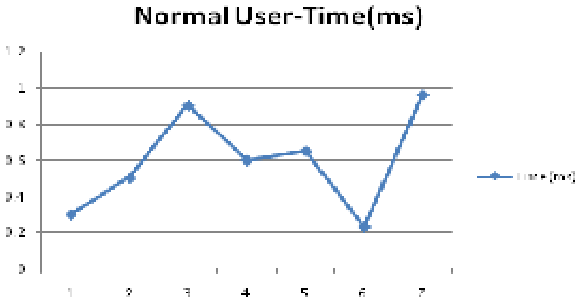

Figure 2: Normal User – Time (ms)

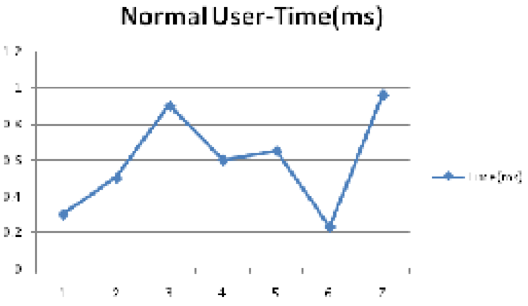

Figure 3: Misbehave User Variation

5.1 Performance:

Collected various empirical performance numbers by implementing Nymble, which verify the linear time and space costs of the various operations and data structures, We use SHA-256 for the cryptographic hash functions.HMAC-SHA-256 for the message authentication MA.AES-256 in CBC-mode for the symmetric encryption Enc and 2,048-bit RSASSA- PSA for the digital signatures Sig. We chose RSA over DSA for digital signatures because of its faster verification speed—in our system, verification occurs more often than signing. We evaluated our system on a 2.2 GHz Intel Core 2 Duo Mac book Pro with 4 GB of RAM. The PM, the NM, and the server were implemented as Mongrel servers. The user portion was implemented as a Firefox 3 extension in JavaScript withXPCOMbindings to the Nymble C++ library. For each experiment relating to protocol performance, we report the average of 10 runs. The evaluation of data structure sizes is the byte count of the marshaled data structures that would be sent over the network.

6.Discussion

IP-address blocking: Our current implementation closely mimics IP-address blocking employed by internet services. There are some inherent limitations to using IP addresses as the scarce resource. The user can circumvent both nymble-based and regular IP- address blocking, subnet-based blocking removes this problem. New privacy challenges emerge, while there is the possibility for modifying our system to support subnet-based blocking.

Other resources: Users of anonymizing networks would be reluctant to use resources that directly reveal their identity .e-mail addresses could provide more privacy, but do not provide proper blacklistability due to frequent change of e-mail addresses by the users. There are other resources like client puzzles, and e-cash. These approaches would limit the number of credentials obtained by a single individual by raising the cost of acquiring credentials. ***Server-specific linkability windows:*** Our system does not support varying linkability windows but does support varying time periods. It is because the PM is not aware of the server of the user's choice, and still it must issue pseudonyms specific to a linkability window. The user use of resources like client puzzles or e-cash would eliminate the need for a PM. The users can obtain nymbles directly from the NM.As such, server-specific linkability windows can be used.
Side-Channel Attacks: Though the current implementation does not protect against side-channel attacks, atleast we are able to minimizing risks. The present implementation of various algorithms assures that the execution time leaks little information that cannot already be inferred from the algorithm's output. Confidential channel does not hide the size of the communication. As such, we have constructed the protocols in such a way that each kind of protocol message is of the same size regardless of the identity or current legitimacy of the user.

7.Conclusion

This comprehensive credential system is called nymble. It 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 disconnecting user as soon as inscribed in the blacklist. We have shown the way of attaining pragmatic values efficiently which is sensitive to the needs of both the user and services. The mainstream acceptance of anonymizing network will be increased because of this work.

References

[1] 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.

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

[3] D. Chaum, "Blind Signatures for Untraceable Payments," Proc. Ann. Int'l Cryptology Conf. (CRYPTO), pp. 199-203, 1982.

[4] 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.

[5] G. Ateniese, D.X. Song, and G. Tsudik, "Quasi-Efficient Revocation in Group Signatures," Proc. Conf. Financial Cryptography, Springer, pp. 183-197, 2002.

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

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

[8] 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.

[9] P.P. Tsang, 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.

[10] P.P. Tsang, 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.

[11] Patrick P.Tsang, Apu Kapadia,"Nymble: Blocking Misbehaving Users In Anonymizing Networks,"Mar-Apr 2011

U.R.V.NANDHINY received the bachelor of Engineering degree in 2006 and pursuing the master of engineering (Software Engineering) .Her research interests are in the area of Networks,Network security ,Datamining U.R.V.Nandhiny B.E,Final year M.E(software engineering) PG Student,Periyar Maniammai University, Thanjavur,TamilNadu, India

M.B.BOSE received the Msc(Software engineering) at noorul islam college of Engineering degree in 2007 and master of engineering (Software Engineering) at pmctw in 2009.His research interests are in the area of Network and network security

He is working as Assistant Professor in Periyar Maniammai University, Thanjavur,Tamilnadu,India

R.SWATHIRAMYA received the bachelor of Engineering degree in 2010 and pursuing the master of engineering(SoftwareEngineering).Her research interests are in the area of Networks,Network security,biometrics, Imageprocessing ,cryptography R.Swathiramya B.E Final year M.E(software engineering) PG Student,Periyar Maniammai University, Thanjavur,TamilNadu, India

P. ELAKIYASELVI received the bachelor of Engineering degree in 2009 and pursuing the master of engineering(SoftwareEngineering).Her research interests are in the area of Networks,Network security,Android Developing mobile applications ,cryptography P.Elakiyaselvi B.E, Final year M.E(software engineering) PG Student,Periyar Maniammai University, Thanjavur,TamilNadu, India

K.LAVANYA received the bachelor of Engineering degree in 2010 and pursuing the master of engineering (Software Engineering).Her research interests are in the area of Networks,Network security,Data mining,Web Technology K.Lavanya B.E,Final year M.E(software engineering) PG Student,Periyar Maniammai University, Thanjavur,TamilNadu, India

P.YATHEESHA received the bachelor of Engineering degree in 2010 and persuing the master's of information technology(Mainframe technology).Her research interests are in the area of Networks,Network security and Mainframe Networks. She is working as Lecturer in ppg institute of Technology Coimbatore,Tamil nadu,India