Blocking Misbehaving Users in Anonymizing Networks

Chandra Chary Sreeramoj,Banoth Rajkumar Rathod , Dr. G. Narsimha

Abstract - Internet services can be accessed privately through anonymizing networks like Tor. A set of routers are used to achieve this in order to hide the identity of client from server. The users of such networks often indulge into malicious activities and cause damage to popular web applications. The administrators of those web sites do block the IP address from which the request comes. This is not the practical solution as the hackers operate through anonymous networks. Blocking a node based on IP address will cau se misbehaving and genuine users to lost access to the web sites. This is the problem in the existing systems and motivation to take up this research work. The proposed system develops a security mechanism that ensures that only the misbehaving users are blackl isted while genuine users and their anonymity are preserved. Even though the misbehaving users are blacklisted, their privacy is still maintained. The experiments revealed that the system is able to block misbehaving users only instead of blocking the node through IP address.

Index Terms: anonymizing networks, misbehaving users, blacklisting,

INTRODUCTION

Anonymizing networks like Tor [13] are able to route traffic via nodes that are independent in distinct administrative domains for hiding IP address of a client. Such networks are misused by certain users unfortunately under the mask of anonymity, users in a repeated manner defaced famous websites like Wikipedia. As administrators of the website are not able to blacklist individual malicious IP addresses of users, they blacklist the whole anonymizing network. This kind of measures removes malicious activity via anonymizing networks at the cost of anonymous access rejection to behaving users.

There are several answers for addressing this problem, each offering some amount of accountability. In case of pseudonymous credential systems [10], [12], [15], [17], users register into websites by making use of pseudonyms that are added to a blacklist if any user attempts to misbehave. The results of this approach are pseudonymity for every user, and lessen the strength of the anonymity that is offered by the anonymizing network.

Group signatures [6], [8] incorporated by Anonymous credential systems. Fundamental group signatures [1], [3], [11] let servers for revoking a user's anonymity who is misbehaving by giving complaint to a group manager. Servers should be able to query the group manager for each authentication, and thus scalability is lacked. Traceable signatures [16] permit the group manager for releasing a trapdoor which allows every signature that is generated by a specific user to be found. This kind of approach does not offer the backward unlinkability [18] which is desired, where accesses of the user prior to the complaint continue to be anonymous. The permission is given by backward unlinkability for what is called as subjective blacklisting, in which servers are able to blacklist users for any reason as the privacy of the user who is blacklisted is considered as risk. Approaches, in contrast with no backward unlinkability are required to pay careful consideration to at what time and why all the connections of a user must be linked, and users must be concerned regarding the issue that whether their behaviors would be judged in a fair manner.

Subjective blacklisting is also better applicable to servers like Wikipedia, if misbehaviors like questionable edits to a webpage are hard for defining in terms of mathematics. In certain systems, misbehavior indeed can be defined in a precise manner. For example, "e-coin" double spending has been treated as misbehavior in anonymous e-cash systems [5], having followed which the user who is offending is de-anonymized. Such kind of systems is able to work for narrow definitions regarding misbehavior alone. It is critical for mapping more complex ideas of misbehavior onto "double spending" or concerned approaches [20].

Through accumulators that are dynamic [7], [19], an operation of revocation leads to a new accumulator as well as public parameters for the group, and remaining various available credentials of the user should be updated, thus it is made impractical. Verifier-local revocation (VLR) [2], [4], [5] is used to fix this inadequacy by having the necessity of the server ("verifier") for performing local updates while revocation alone. VLR has the necessity of large computation at the server which is linear in the blacklist size. For instance, for a blacklist having thousand entries, every authentication would consider tens of seconds, 2 an excessive cost in practice. In contrast, the proposed scheme considers the server around 1 millisecond per authentication that is several thousand times quicker than VLR. It is believed that these small overheads would incentivize servers for adopting such a solution when it is weighed against the potential advantages of anonymous publishing like whistle-blowing.

A secure system is presented in the paper, that provides each of the below properties: anonymous authentication, subjective blacklisting, backward unlinkability, rate-limited anonymous connections, speeds of fast authentication and auditability of revocation (where users are able to verify if they are blacklisted), and even the Sybil attack [14] is addressed for making it deployment practical.

PROPOSED SOLUTION

The proposed solution to the problem of blacking misbehaving users has properties such as addressing Sybil attack [14], revocation auditability, rate-limited anonymous connections, fast authentication speeds, subjective blacklisting, backward unlinkability, and anonymous authentication. In the proposed system security is provided when users connect to web sites. Users get pseudonyms from Pseudonym Manager in order to gain access to web sites. These pseudonyms help in gaining anonymous access to web sites. The system ensures that genuine users connect to web sites and their anonymity is preserved. At the same time misbehaving users are kept in blacklist. This paper contributes features such as blacklisting anonymous users; practical performance; and open source implementation.

- *Department of Computer Science Engineering Phd. Research scholar JNTUH, Kukatpally, Hyd Mail ID: naaniraj@gmail.com, Mob: 9849731856*
- *Assoc. Prof. Department of Computer Science and Engineering JNTUH, Kukatpally, Hyderabad Mail ID:* Narsimha06@gmail.com *Mob:990885308*

ARCHITECTURE OF PROPOSED SYSTEM

The following figure shows high level overview of the system. It describes the complete security mechanism and the process of blacklisting misbehaving users. The components involved in this architecture are pseudonym manager, nimble manager, user and server.

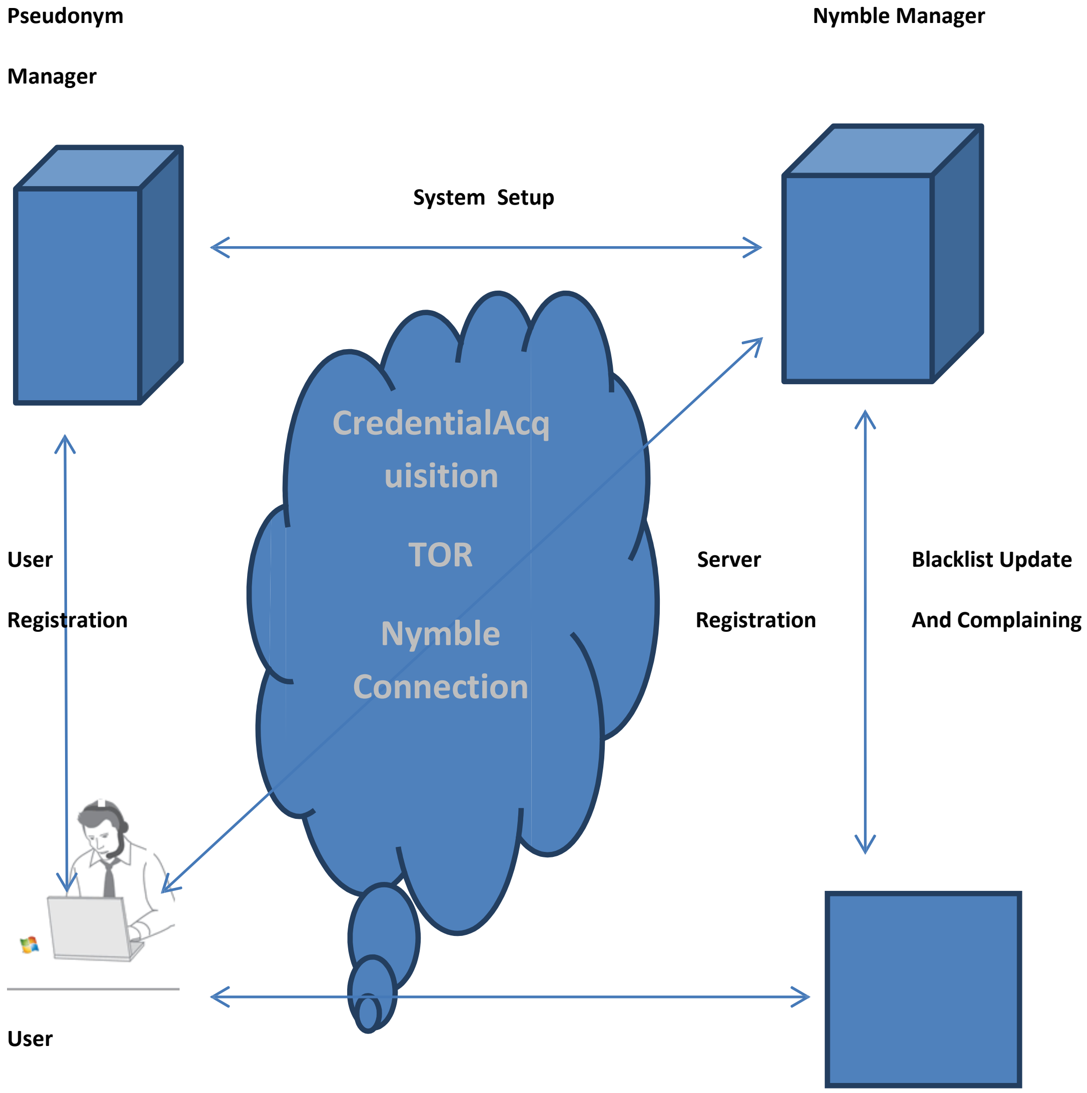

Fig. 1 shows security architecture of the proposed sts

As can be seen in fig. 1, the users' user can have secure access to web server. First of all user connects to PM (Pseudonym Manager) in order to obtain pseudonyms. At that time the user does not inform to PM to which server he is going to connect to get web sites. This is a single step procedure followed by users.

Nymble Manager

Once user gets pseudonyms from PM, he is able to connect to nymble manager. User requests to NM are pseudonyms. The NM is capable of generating nymbles based on pseudonyms. The nymbles created are specific to user-server pair. They won't work for other servers.

Time Bound Nymbles

Specific time periods are bound to nymble tickets. The time is divided into likability windows of duration W. Depending on the user behavior, the user is treated. When system suspects that the user is misbehaving, the user is kept in blacklist temporarily for some time. After wards, user can be removed from black list automatically. A special protocol named NTP is used to calculate the current likability window and time period.

Blacklisting a User

When user misbehaves, the server can link future connection from this user within the current linkability window. Only for some time period the misbehaving user is blacklisted. The users past actions can be linkable. The present misbehavior can span on the Window to some extent. Afterwards the user must be made genuine user and allow access to details. In this case the blacklisting will be effective only for 24 years.

Notification

The user is notified when he is kept in black list. Irrespective of these, users want to have anonymous access to web sites
through network. When users misbehave, they are kept in blacklist. At the same time, the system has to notify that user about his blacklist status. Such blacklist is signed by NM cryptographically.

SECURITY MODEL

The proposed system aims at security goals such as blacklistability, rate-limiting, nonframability, and anonymity. Blacking misbehaving users is known as blacklistability; honest users are not denied access to servers is known as nonframability; with a single time period honest users can nymble-connect only once; anonymity protects honest users.

DATA STRUCTURES

In order to implement system many data structures are used. They are described in the following sub sections. Algorithms are also described in those sections.

Pseudonyms

Every pseudonym has two parts. They are nym and mac. Nym is pertaining to user identity while mac is a MAC that the NM uses in order to check correctness of pseudonym.

ALGORITHM	1.PMCreate Pseudynoum
INPUT	(Uid,w)Ɛ H×N
OUTPUT	Pnym Ɛ P
STEPS	1. Extract nymKeyp,macKeyNP from pmState
	2.nym :=MA.Mac(uid∥w ,nymKeyp)
	3.mac:=MA.Mac(nym∥w,macKeyNP)
	4. return pnym:=(nym,mac)

Table 1 shows algorithm1

ALGORITHM	2.NMVerify Pseudynoum
INPUT	(pnym,w)Ɛ P×N
OUTPUT	bƐ {true,false}
STEPS	1. Extract macKeyNP from nmState
	2. (nym ,mac):=pnym
	3. return mac=MA.Mac(nym∥w,macKeyNP)

Table2 shows Algorithm2

Seeds and Nymbles

For a specific time period, nymble is a pseudorandom number which represents an identifier. Such nymbles are not linkable unless the user is blacklisted. They are presented as part of nymble ticket. Seeds are numbers used to generate nymbles. Two distinct cryptographic hash functions such as f and g are used in nymble construction. Thus future nymbles can be easily computed using seed values. When a seed for a specific period of time is obtained, the nymbles created prior to that time period remain unilnkable.

NYMBLE TICKETS and CREDENTIALS

Credential is something which has all nymbles tickets for a particular time window pertaining to specific user-server. Algorithm 3 provides steps as to how to generate a credential when a request for it is made.

ALGORITHM	3.NMCreate Credential
INPUT	(pnym,sid, w)Ɛ P×H×N
OUTPUT	Cr edƐ D
STEPS	1. Extract macKeyNPS;macKeyN;seedKeyN;encKeyNfrom Keys in nmState
	2. Seed0:f(Mac(pnymǁsidǁw,seedKeyN))
	3. nymble*:=g(seed0)
	4.for t from 1 to L do
	5.seedt :=f(seedt-1)
	6.nymble:=g(seedt)
	7.ctxt:=Enc.Encrypt(nymble*ǁseedt,encKeyN)
	8.ticket:=sidǁtǁwǁnymbleǁctxt
	9.macN :=MA.Mac(ticket,macKeysN)
	10.macNS:=MA.Mac(ticket,mac,macKeyNS)
	11.tickets[t]:=(t,nymble,ctxt,macN,macNS)
	12.return cred:=(nymble*,tickets)

Table 3 shows algorithm3

ALGORITHM	4.NMVerify ticket
INPUT	(Sid,t,w,ticket)Ɛ T×N×N
OUTPUT	b Ɛ {true,false}
STEPS	1. Extract macKeyNPSfromnmState
	2. (.,nymble,ctxt,macN,macNS):=ticket
	3. content:=sidǁtǁwǁnymbleǁctxt
	4.return macN =MA.Mac(content,macKeyN)

Table 4 shows algorithm 4

ALGORITHM	5ServerVerify Ticket
INPUT	(t,w,ticket)Ɛ T×N×N
OUTPUT	b Ɛ {true,false}
STEPS	1. Extract sid, macKeyNS from svr State
	2. (.,nym ble,ctxt,macN,macNS):=ticket
	3. content:=sidǁtǁwǁnymbleǁctxt
	4.return macN =MA.Mac(content,macKeyN)

Table 5 shows algorithm 5

Blacklists

For all the nymbles, server has complained, a black list is created. This black list can be quickly checked by users to find their status in the blacklist.

PERFORMANCE EVALUATION

The proposed system has been implemented and evaluated. The details are described in the following sub sections.

Experimental Setup and Implementation Details

The proposed system has been implemented using Java programming language. The system has OS that is Microsoft Windows XP Professional with 2 GB RAM and Intel Core 2 Dual processor. Experiments are done and statistics are populated. They are used in generating graphs shown below.

Experimental Results

The empirical results of proposed work are described here with the help of graphs. Fig. 2 shows number of entries plotted in X and Size in KB is plotted in Y coordinated.

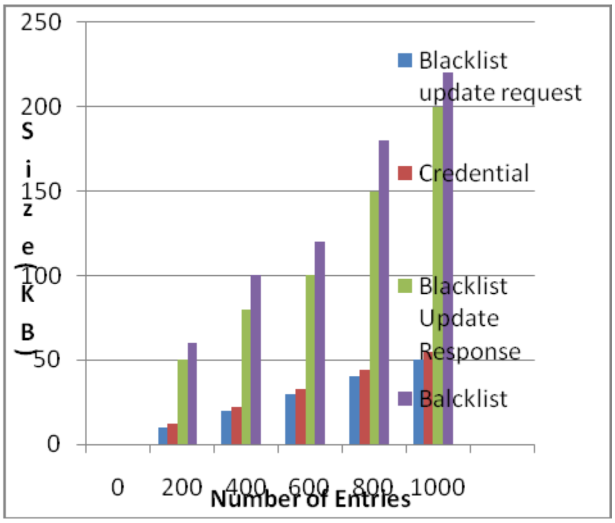

Fig. 1 shows the size statistics based on the number of entries.

As can be seen in fig. 1, the X-Axis represents number of entries in the blacklist update requests, tickets in credential, nymbles in the blacklist tokens and seeds in the blacklist update response and nymbles in the blacklist.

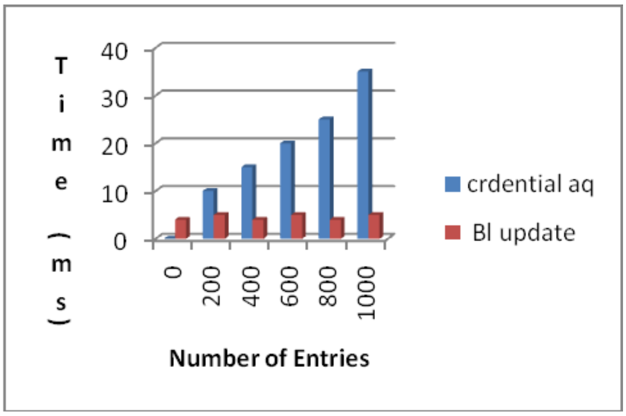

Fig. 2shows the blacklist updates

As seen in fig. 2, it is evident that the nymbles performance. Blacklist updates take many milli seconds, and credentials can be
generated in 9 ms for suggested parameter L = 288.

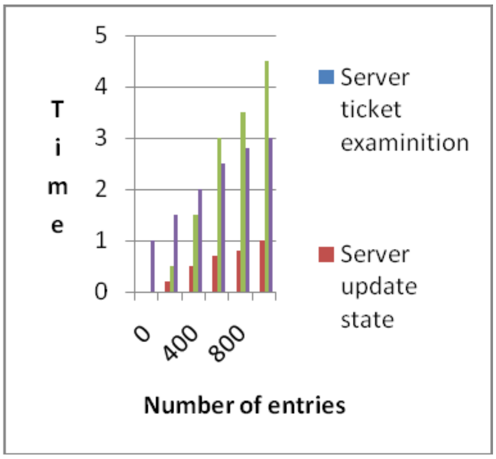

Fig. 3 shows the performance of nymbles

As can be seen in fig. 3, the bottleneck operation of server ticket examination is less than 1 ms and validating blacklist takes the user only a few ms.

SECURITY ANALYSIS

The proposed system security analysis considers blacklistability, nonframability, anonymity, and across multiple linkability windows. Blacklistability has been tested and it is working fine and the user is kept in blacklist for some time and then once time window changed, it is changed again. Nonframebility has ensured that an adversary can't forge tickets. Anonymity ensured that genuine users are not denied access to web sites while the misbehaving users are kept in blacklist at least for the completion of current time window.

CONCLUSION

A comprehensive credential system is proposed that can be useful for adding an accountability layer to any well known anonymizing network. Servers are able to blacklist users who
are misbehaving and maintain privacy of them, and it is showed that it is possible to attain those properties in a manner which is practical, effective, as well as sensitive to requirements of both users as well as services.

REFERENCES

[1] G. Ateniese, J. Camenisch, M. Joye, and G. Tsudik, "A Practicaland Provably Secure Coalition-Resistant Group Signature,Scheme," Proc. Ann. Int'l Cryptology Conf. (CRYPTO), Springer,pp. 255-270, 2000.

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

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

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

[5] E. Bresson and J. Stern, "Efficient Revocation in Group Signatures,"Proc. Conf. Public Key Cryptography, Springer, pp. 190-206,2001.

[6] J. Camenisch and A. Lysyanskaya, "An Efficient System for Non-Transferable Anonymous Credentials with Optional

AnonymityRevocation," Proc. Int'l Conf. Theory and Application of CryptographicTechniques (EUROCRYPT), Springer, pp. 93-118, 2001.

[7] J. Camenisch and A. Lysyanskaya, "Dynamic Accumulators andApplication to Efficient Revocation of Anonymous Credentials,"Proc. Ann. Int'l Cryptology Conf. (CRYPTO), Springer, pp. 61-76,2002.

[8] J. Camenisch and A. Lysyanskaya, "Signature Schemes andAnonymous Credentials from Bilinear Maps," Proc. Ann. Int'lCryptology Conf. (CRYPTO), Springer, pp. 56-72, 2004.

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

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

[11] D. Chaum and E. van Heyst, "Group Signatures," Proc. Int'l Conf.Theory and Application of Cryptographic Techniques (EUROCRYPT),
pp. 257-265, 1991.

[12] I. Damga°rd, "Payment Systems and Credential Mechanisms withProvable Security Against Abuse by Individuals," Proc. Ann. Int'lCryptology Conf. (CRYPTO), Springer, pp. 328-335, 1988.

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

[14] J.R. Douceur, "The Sybil Attack," Proc. Int'l Workshop on Peer-to-Peer Systems (IPTPS), Springer, pp. 251-260, 2002.

[15] J.E. Holt and K.E. Seamons, "Nym: Practical Pseudonymity forAnonymous Networks," Internet Security Research Lab TechnicalReport 2006-4, Brigham Young Univ., June 2006.

[16] 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.

[17] A. Lysyanskaya, R.L. Rivest, A. Sahai, and S. Wolf, “PseudonymSystems,” Proc. Conf. Selected Areas in Cryptography, Springer,pp. 184-199, 1999.

[18] T. Nakanishi and N. Funabiki, “Verifier-Local Revocation Group Signature Schemes with Backward Unlinkability from BilinearMaps,” Proc. Int’l Conf. Theory and Application of Cryptology andInformation Security (ASIACRYPT), Springer, pp. 533-548, 2005.268 IEEE TRANSACTIONS ON DEPENDABLE AND SECURE COMPUTING, VOL. 8, NO. 2, MARCH-APRIL 2011

[19] L. Nguyen, “Accumulators from Bilinear Pairings and Applications,”Proc. Cryptographer’s Track at RSA Conf. (CT-RSA), Springer,pp. 275-292, 2005.

[20] I. Teranishi, J. Furukawa, and K. Sako, “k-Times AnonymousAuthentication (Extended Abstract),” Proc. Int’l Conf. Theory andApplication of Cryptology and Information Security (ASIACRYPT),Springer, pp. 308-322, 2004.