



International Journal of Engineering, Business and Enterprise Applications (IJEBA)

www.iasir.net

NYMBLE: Protecting the Privacy of Users in Anonymous Networks and Blacklisting Misbehaving Users

R Anto Arockia Rosaline

Assistant Professor

Department of Information Technology

Rajalakshmi Engineering College, Chennai.

E-mail: antoarockiarosaline.r@rajalakshmi.edu.in

V. Deepti Sarojini Benitta

Department of Information Technology

Rajalakshmi Engineering College, Chennai.

E-mail: deeptiben@gmail.com

Abstract: Anonymizing networks hide the client's IP address and allow the client to access the internet. It protects the privacy of users but unfortunately some users have misused such networks for abusive purposes. Website administrators block the IP addresses of misbehaving users and as a result they block all the known exit nodes of the anonymizing networks, denying anonymous access to misbehaving and behaving users alike. Since the server does not identify individual user's activities all the users are blocked from accessing resources of the server from the particular anonymous network. In the proposed system the users are identified individually without revealing their identity. Nymble is the proposed system in which the servers can "blacklist" misbehaving users, thereby blocking users without compromising their anonymity. The system detects the misbehaving users and adds them to the blacklist. Thus the server can blacklist the misbehaving users without knowledge of their IP address and allows behaving users to connect anonymously. Those of the users in the blacklist are blocked from accessing the resources for a specified time that is set by the administrators. The proposed system has several important properties which overcome the drawbacks of the existing system. The properties are anonymous authentication, backward unlinkability, subjective blacklisting, fast authentication speeds, blacklist sharing, rate limited anonymous connections, revocation auditability and also addresses Sybil attacks.

Keywords: Anonymous, backward unlinkability, blacklist, digital signatures, revocation.

I. Introduction

Anonymizing networks such as Tor [21] route traffic through independent nodes in separate administrative domains to hide a client's IP address. Unfortunately, some users have misused such networks - under the cover of anonymity, users have repeatedly defaced popular websites such as Wikipedia. Since website administrators cannot blacklist individual malicious users' IP addresses, they blacklist the entire anonymizing network. Such measures eliminate malicious activity through anonymizing networks at the cost of denying anonymous access to behaving users. In other words, a few "bad apples" can spoil the fun for all. (This has happened repeatedly with Tor) There are several solutions to this problem, each providing some degree of accountability. In pseudonymous credential systems [3], [4], [9], [10], users log into websites using pseudonyms, which can be added to a blacklist if a user misbehaves. Unfortunately, this approach results in pseudonymity for all users, and weakens the anonymity provided by the anonymizing network.

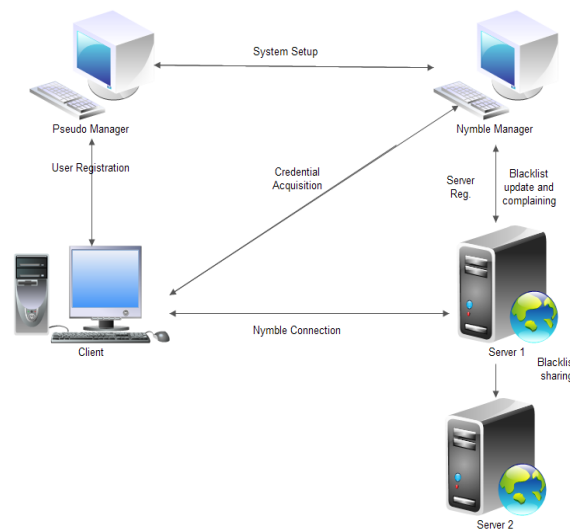
Anonymous credential systems [3], [10] employ group signatures. Basic group signatures [13], [14], [15] allow servers to revoke a misbehaving user's anonymity by complaining to a group manager. Servers must query the group manager for every authentication, and thus lacks scalability. Traceable signatures [6] allow the group manager to release a trapdoor that allows all signatures generated by a particular user to be traced; such an approach does not provide the backward unlinkability [3] that we desire, where a user's accesses before the complaint remain anonymous. Backward unlinkability allows for subjective blacklisting, where servers can blacklist users for whatever reason since the privacy of the blacklisted user is not at risk. In contrast, 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. Subjective blacklisting is also better suited to servers such as Wikipedia, where misbehaviors such as questionable edits to a webpage, are hard to define in mathematical terms. In some systems, misbehavior can indeed be defined precisely. For instance, double-spending of an "e-coin" is considered a misbehavior in anonymous e-cash systems, following which the offending user is deanonymized. Unfortunately, such systems work for only narrow definitions of misbehavior — it is difficult to map more complex notions of misbehavior onto "double spending" or related approaches.

With dynamic accumulators [3], a revocation operation results in a new accumulator and public parameters for the group, and all other existing users' credentials must be updated, making it impractical. Verifier-local revocation (VLR) [14], [16] fixes this shortcoming by requiring the server ("verifier") to perform only local updates during revocation. Unfortunately, VLR requires heavy computation at the server that is linear in the size of the blacklist. For example, for a blacklist with 1,000 entries, each authentication would take tens of seconds.

II. PROPOSED SOLUTION

Nymble is the proposed system, which provides all the following properties: anonymous authentication, backward unlinkability, subjective blacklisting, fast authentication speeds, rate-limited anonymous connections, revocation auditability (where users can verify whether they have been blacklisted), and also addresses the Sybil attack to make its deployment practical. In Nymble, users acquire an ordered collection of nymbles, a special type of pseudonym, to connect to websites. 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 remains unlinkable. Servers can therefore blacklist anonymous users without knowledge of their IP addresses while allowing behaving users to connect anonymously. This system ensures that users are aware of their blacklist status before they present a nymble, and disconnect immediately if they are blacklisted. Although this work applies to anonymizing networks in general, we consider Tor for purposes of exposition. 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. The cryptographic primitives that would be used in the proposed solution are cryptographic hash functions, message authentication, symmetric-key encryption and digital signatures.

Figure 1 Architecture Diagram



III. AN OVERVIEW TO NYMBLE

A. Resource Based Blocking

To limit the number of identities a user can obtain (called the Sybil attack), the Nymble system binds nymbles to resources that are sufficiently difficult to obtain in great numbers. For example, one can use the IP addresses as the resource in our implementation, but our scheme generalizes to other resources such as email addresses, identity certificates, and trusted hardware.

B. 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 anonymizing network), as shown in the above Figure. Pseudonyms are deterministically chosen based on the controlled resource, ensuring that the same pseudonym is always issued for the same resource. Note that the user does not disclose what server he or she intends to connect to, and the PM's duties are limited to mapping IP addresses (or other resources) to pseudonyms.

C. 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). A user's requests to the NM are therefore pseudonymous, and nymbles are generated using the user's pseudonym and the server's identity. These nymbles are thus specific to a particular user-server pair. Nevertheless, as long as the PM and the NM do not collude, the Nymble system cannot identify which user is connecting to what server; the NM knows only the pseudonym-server pair, and the PM knows only the user identity-pseudonym pair. To provide the requisite cryptographic protection and security properties, the NM encapsulates nymbles within nymble tickets. Servers wrap seeds into linking tokens used to link future nymble tickets.

D. Blacklisting a Misbehaving User

If a user misbehaves, the server may link any future connection from this user within the current linkability window (e.g., the same day). As part of the complaint, the server presents the nymble ticket of the misbehaving user and obtains the corresponding seed from the NM. The server is then able to link future connections by the same user. Even though misbehaving users can be blocked from making connections in the future, the users' past connections remain unlinkable, thus providing backward unlinkability and subjective blacklisting.

E. Notifying the User 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, 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. Since the blacklist is cryptographically signed by the NM, the authenticity of the blacklist is easily verified if the blacklist was updated in the current time period (only one update to the blacklist per time period is allowed).

IV. NYMBLE CONSTRUCTION

A. System Setup

During setup, the NM and the PM interact as follows.

- 1) Both of the systems initialise their state and refresh their memory values.
- 2) NM executes message authentication – key generation in order to generate a unique key to encrypt and decrypt the pseudonym.
- 3) Once the keys are exchanged the system setup phase ends.

B. Server Registration

In order to participate in the nymble system, the servers must register their server ids and their names along with any of the linked server names if present. The servers register all the details with the NM. The NM acknowledges the receipt of the details along with the encryption key that will be used to encrypt the session ids.

C. User Registration

The protocol between user and pseudonym is as follows.

- 1) The user using its user id such as IP address contacts the PM.
- 2) The PM verifies its id and issues the pseudonym by using the algorithm pseudorandom generator.
- 3) Then the user can contact the NM using the encrypted pseudonym and server name for further access to server.

D. Nymble Connection Establishment

To establish a connection to the server the user must first contact the NM using its pseudonym and desired server name. The following steps are carried out during connection establishment.

- 1) Blacklist validation:

The server sends the blacklist status to the user along with its signing keys. The signing keys are produced by the message authentication code. The verifying algorithms are used to verify the blacklist status that was updated by the NM.

- 2) Ticket examination:

The NM before issuing the nymble session id verifies the pseudonym if it was signed by the PM. The keys which were shared during the system setup is used to verify the pseudonym.

E. Access Logging and Filing for Complaint

If both the user and the server terminate with success in the Nymble-connection Establishment described above, the server may start serving the user over the same channel. The server records ticket and logs the access during the session for a potential complaint in the future. If at some later time the server desires to blacklist the user behind a Nymble-connection, during the establishment of which the server collected ticket from the user, the server files a complaint by appending ticket to cmplt-tickets in its sever state. Filed complaints are batched up. They are processed during the next blacklist update.

F. Blacklist Update

Servers update their blacklists for the current time period for two purposes. First, as mentioned earlier, the server needs to provide the user with its blacklist (and blacklist certificate) for the current time period during a Nymble connection establishment. Second, the server needs to be able to blacklist the misbehaving users by processing the newly filed complaints (since last update). The procedure for updating blacklists (and their certificates) differs depending on whether complaints are involved. When there is no complaint (i.e., the server's cmplt-tickets is empty), blacklists stay unchanged; the certificates need only a "light refreshment." When there are complaints, on the other hand, new entries are added to the blacklists and certificates need to be regenerated.

G. Periodic Update

At the end of a given time period the servers and NM performs a refresh in order to clear all the mentioned blacklist members. During the performance of refresh all the users who were blacklisted is removed. This is done in order to include the concept of what is called as "forgiveness time".

V. Implementation and experimental setup

JavaScript can be used to implement the above system due to its in built properties and characteristics. Using SHA-256 for the cryptographic hash functions; HMAC-SHA-256 for the message authentication MA; AES-256 in CBC-mode for the symmetric encryption and 2048-bit RSA SSA-PSA for the digital signatures is recommended. Choosing RSA over DSA for digital signatures because of its faster verification speed—in this system, verification occurs more often than signing. Assume that the PM and NM will not be compromised at any cost. The PM and NM can be implemented as hosts or servers. In this system PM and NM are to be implemented as servers. The system requires 2.2GHz Intel Pentium Dual-Core with 4GB RAM.

VI. CONCLUSIONS

We have proposed 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 it is seen how these properties can be attained in a way that is practical, efficient, and sensitive to needs of both users and services. Hope that this proposed 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.

ACKNOWLEDGEMENT

We would like to thank Dr.G.Poonkuzhali,Head of the Department, Department of Information Technology, Rajalakshmi Engineering College, for her encouragement and support.

REFERENCES

- [1] G. Ateniese, J. Camenisch, M. Joye, and G. Tsudik. A Practical and Provably Secure Coalition-Resistant Group Signature Scheme. In CRYPTO, LNCS 1880, pages 255–270. Springer, 2000.
- [2] G. Ateniese, D. Song and G. Tsudik. Quasi-Efficient Revocation of Group Signatures. In Financial Cryptography, LNCS 2357, pages 183–197. Springer, 2002.
- [3] J. Camenisch and A. Lysyanskaya. Dynamic Accumulators and Application to Efficient Revocation of Anonymous Credentials. In CRYPTO, LNCS 2442, pages 61–76. Springer, 2002.
- [4] P. Tsang, M. H. Au, A. Kapadia and S. W. Smith. Blacklistable Anonymous Credentials: Blocking Misbehaving Users without TTPs. In CCS '07: Proceedings of the 14th ACM conference on Computer and communications security, pages 72–81, New York, NY, USA, 2007. ACM.
- [5] C. Johnson, A. Kapadia, P. Tsang and S. W. Smith. Nymble: Anonymous IP-Address Blocking. In Privacy Enhancing Technologies, LNCS 4776, pages 113–133. Springer, 2007.
- [6] A. Kiayias, Y. Tsioumis and M. Yung. Traceable Signatures. In EUROCRYPT, LNCS 3027, pages 571–589. Springer, 2004.
- [7] S. Even, O. Goldreich and S. Micali. On-Line/Off-Line Digital Signatures. In CRYPTO, LNCS 435, pages 263–275. Springer, 1989.
- [8] S. Goldwasser, S. Micali and R. L. Rivest. A Digital Signature Scheme Secure Against Adaptive Chosen Message Attacks. In SIAM J. Comput., 17(2):281–308, 1988.
- [9] A. Lysyanskaya, R. L. Rivest, A. Sahai and S. Wolf. Pseudonym Systems. In Selected Areas in Cryptography, LNCS 1758, pages 184–199. Springer, 1999.
- [10] J. Camenisch and A. Lysyanskaya. An Efficient System for Non-transferable Anonymous Credentials with Optional Anonymity Revocation. In EUROCRYPT, LNCS 2045, pages 93–118. Springer, 2001.
- [11] D. Chaum. Blind Signatures For Untraceable Payments. In CRYPTO, pages 199–203, 1982.
- [12] Teranishi, J. Furukawa and K. Sako. k-Times Anonymous Authentication. In ASIACRYPT, LNCS 3329, pages 308–322. Springer, 2004.
- [13] M. Bellare, H. Shi and C. Zhang. Foundations of Group Signatures: The case of Dynamic Groups. In CT-RSA, LNCS 3376, pages 136–153. Springer, 2005.
- [14] D. Boneh and H. Shacham. Group Signatures with Verifier-Local Revocation. In ACM Conference on Computer and Communications Security, pages 168–177. ACM, 2004.
- [15] E. Bresson and J. Stern. Efficient Revocation In Group Signatures. In Public Key Cryptography, LNCS 1992, pages 190–206. Springer, 2001.
- [16] P. Tsang, A. Kapadia, C. Cornelius and S. W. Smith. Nymble: Blocking Misbehaving Users in Anonymizing Networks. In IEEE Transactions on Dependable And Secure Computing, VOL 8, March- April 2011.
- [17] A. Juels and J. G. Brainard. Client Puzzles: A Cryptographic Countermeasure Against Connection Depletion Attacks. In NDSS. The Internet Society, 1999.

- [18] S. Micali. NOVOMODO: Scalable Certificate Validation and Simplified PKI Management. In 1st Annual PKI Research Workshop - Proceeding, April 2002.
- [19] P. P. Tsang, M. H. Au, A. Kapadia, and S. W. Smith. PEREA: Towards Practical TTP-Free Revocation in Anonymous Authentication. In ACM Conference on Computer and Communications Security, pages 333–344. ACM, 2008.
- [20] J. E. Holt and K. E. Seamons. Nym: Practical Pseudonymity for Anonymous Networks. Internet Security Research Lab Technical Report 2006-4, Brigham Young University, June 2006.
- [21] R. Dingledine, N. Mathewson, and P. Syverson. Tor: The Second-Generation Onion Router. In Usenix Security Symposium, pages 303–320, Aug. 2004.