RESEARCH ARTICLE OPEN ACCESS

NYMBLE: Blocking Misbehaving Users in Anonymizing Networks

[1]R.Ravikumar, [2]J.Ramesh Kumar
[1]Asst.professor, Dept.of.Computer Science, Tamil University, Thanjavur-613010.
[2]Research Scholar, Dept.of.Computer Science, Tamil University, Thanjavur-613010.

Abstract:

Nymble, a system in which servers can blacklist misbehaving users, thereby blocking users without compromising their anonymity. Our system is thus agnostic to different servers' definitions of misbehavior servers can blacklist users for whatever reason, and the privacy of blacklisted users is maintained. In pseudonymous credential systems users log into Web sites using pseudonyms, which can be added to a blacklist if a user misbehaves. Anonymous credential systems employ group signatures. Basic group signatures allow servers to revoke a misbehaving user's anonymity by complaining to a group manager. Anonymizing networks such as Tor allow users to access Internet services privately by using a series of routers to hide the client's IP address from the server. The success of such networks, however, has been limited by users employing this anonymity for abusive purposes such as defacing popular Web sites. Web site administrators routinely rely on IP-address blocking for disabling access to misbehaving users, but blocking IP addresses is not practical if the abuser routes through an anonymizing network. As a result, administrators block all known exit nodes of anonymizing networks, denying anonymous access to misbehaving and behaving users alike. a secure system called Nymble, which provides anonymous authentication, backward unlinkability, subjective blacklisting, fast authentication speeds, rate-limited anonymous connections, revocation auditability that is the users can verify whether they have been blacklisted, Nymble thus represents a practical solution for blocking misbehaving users of anonymizing networks. 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. We assume the PM has knowledge about Tor routers, and can ensure that users are communicating with it directly. Pseudonyms are deterministically chosen based on the controlled resource, ensuring that the same pseudonyms always issued for the same resource.

Keywords — **Nymble, anonymizing networks, symmetric cryptography, blocking.**

I. INTRODUCTION

ANONYMIZING networks such as Tor 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 Web sites such as Wikipedia. Since Web site administrators cannot blacklist individual malicious users' IP addresses, they blacklist the entire anonymizing network. The success of such networks, however, has been limited by users employing this anonymity for Abusive purposes such as defacing popular Web sites. Web site administrators routinely rely on IP-address blocking for disabling access to misbehaving users, but blocking IP addresses is not practical if the abuser routes through an anonymizing network. As a result,

administrators block all known exit nodes of anonymizing networks, denying anonymous access to misbehaving and behaving users alike.

There are several solutions to this problem, each providing some degree of accountability. In pseudonymous credential systems, users log into Web sites 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 employ group signatures. Basic group signatures, 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 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 that we desire, where a user's accesses before the complaint remain anonymous. Backward unlinkability allows for what we call 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.

1.1.EXISTING SYSTEM

Anonymizing networks such as Tor allow users to access Internet services privately by using a series of routers to hide the client's IP address from the server. The success of such networks, however, has been limited by users employing this anonymity for abusive purposes such as defacing popular Web sites. Web site administrators routinely rely on IP-address blocking for disabling access to misbehaving users, but blocking IP addresses is not practical if the abuser routes through an anonymizing network. As a result, administrators block all known exit nodes of anonymizing networks, denying anonymous access to misbehaving and behaving users alike.

1.2.EXISTING SYSTEM DISADVANTAGES

- Unfortunately, this approach results in pseudonymity for all users, and weakens the anonymity provided by the anonymizing network.
- Servers must query the group manager for every authentication, and thus, lacks scalability.
- User must have all their connections linked, and users must worry about whether their behaviors will be judged fairly.

1.3. PROPOSED SYSTEM

We present a secure system called Nymble, which provides anonymous authentication, backward unlinkability, subjective blacklisting, fast authentication speeds, rate-limited anonymous connections, revocation auditability that is the users can verify whether they have been blacklisted, Nymble thus represents a practical solution for blocking misbehaving users of anonymizing networks.

1.4.PROPOSED SYSTEM ADVANTAGES

- Our system ensures that users are aware of their blacklist status before they present a nymble, and disconnect immediately if they are blacklisted.
- In our system, the user can download the server's blacklist and verify her status. If blacklisted, the user disconnects immediately.

ANONYMIZING networks such as Tor 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 Web sites such as Wikipedia. Since Web site administrators cannot blacklist individual malicious users' IP addresses, they blacklist the entire anonymizing network.

II.PROBLEM DEFINITION

Our system ensures that users are aware of their blacklist status before they present a nymble, and disconnect immediately if they are blacklisted.

2.1.METHODOLOGIES

A methodology is the process of analyzing the Nymble: Blocking Misbehaving Users In Anonymizing Networks.

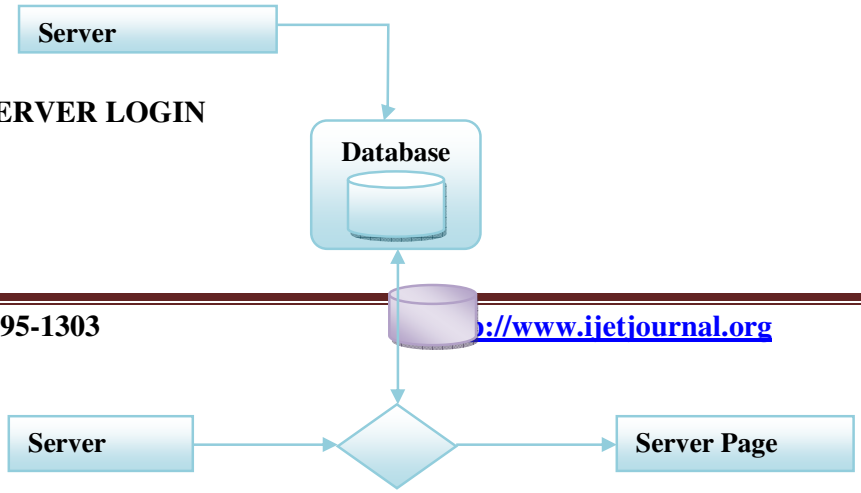
2.2. MODULES NAME

- Server Registration
- User Registration
- Pseudonym Manager
- Nymble Manager
- Blacklist Update

2.3.MODULE DESCRIPTION

SERVER REGISTRATION

To participate in the Nymble system, a server with identity Sid initiates a type-Auth channel to the NM, and registers with the NM according to the Server Registration protocol below. Each server may register at most once in any likability window. Logins may be used to provide credentials when creating a client connection. Whether or not logins are required depends on the method calls used to start the server or create the connection. For example, you might need logins for pooling. If you do not use logins, you must track and specify the user credentials manually.

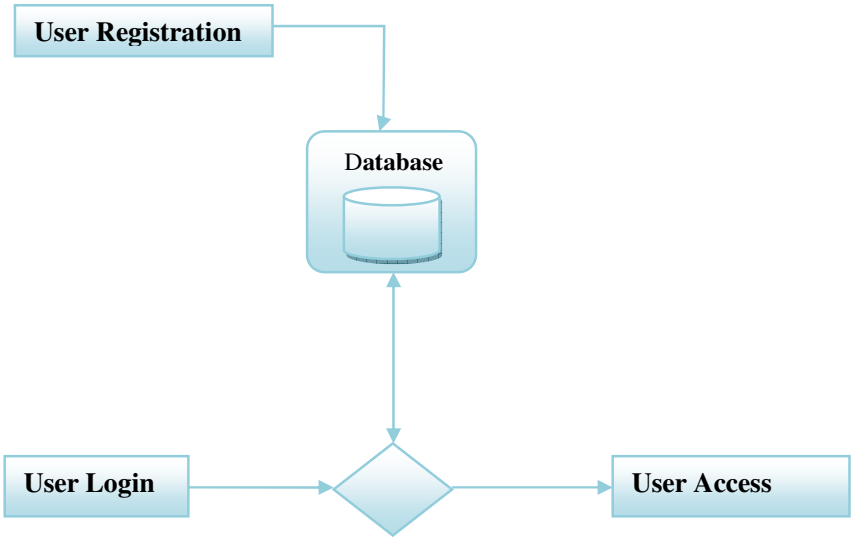


Login Verification

USER REGISTRATION

A user with identity uid must register with the PM once in each likability window. To do so, the user initiates a type- Basic channel to the PM, followed by the User Registration protocol escribed below. A login generally requires the user to enter two pieces of information, first a user name and then a password. This information is entered into a login window on a GUI (graphical user interface). A user name, also referred to as an account name, is a string (i.e., sequence of characters) that uniquely identifies a user. User names can be the same as or related to the real names of users, or they can be completely arbitrary. A password is likewise a string, but it differs from a user name in that it is intended to be kept a secret that is known only to its use.

USER LOGIN



Login Verification

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. We assume the PM has knowledge about Tor routers, and can ensure that users are communicating with it directly. Pseudonyms are deterministically chosen

based on the controlled resource, ensuring that the same pseudonyms always issued for the same resource.

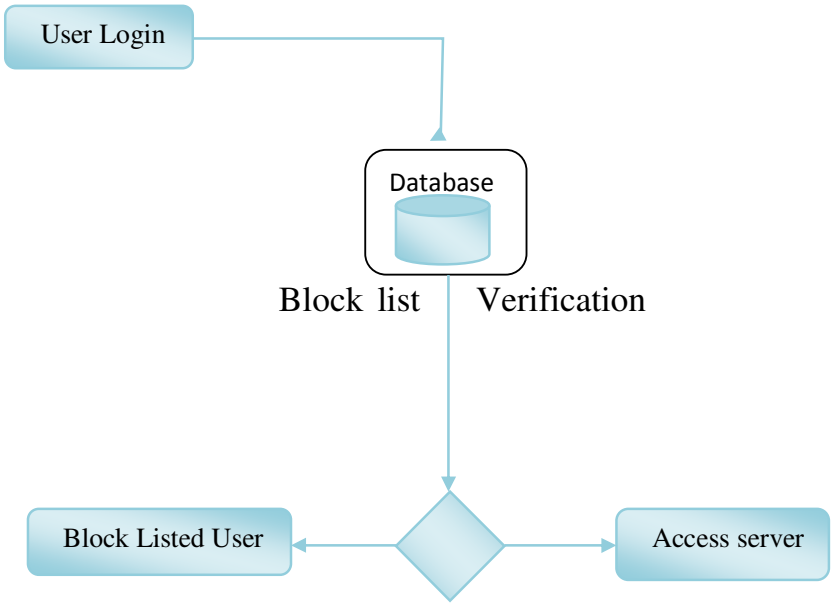
NYMBLE MANAGER

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.

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).

BLOCK LIST



SERVER REGISTRATION

Input: Server Register to Nymble

Output: Nymble Accept the registration

USER REGISTRATION

Input: User Register to Pseudonym Manager

Output: Pseudonym Manager Accept the registration

PSEUDONYM MANAGER

Input: Pseudonym Manager provide Pseudonym

Output: User gets the Pseudonym

NYMBLE MANAGER

Input: Give Pseudonym name to Nymble Manager

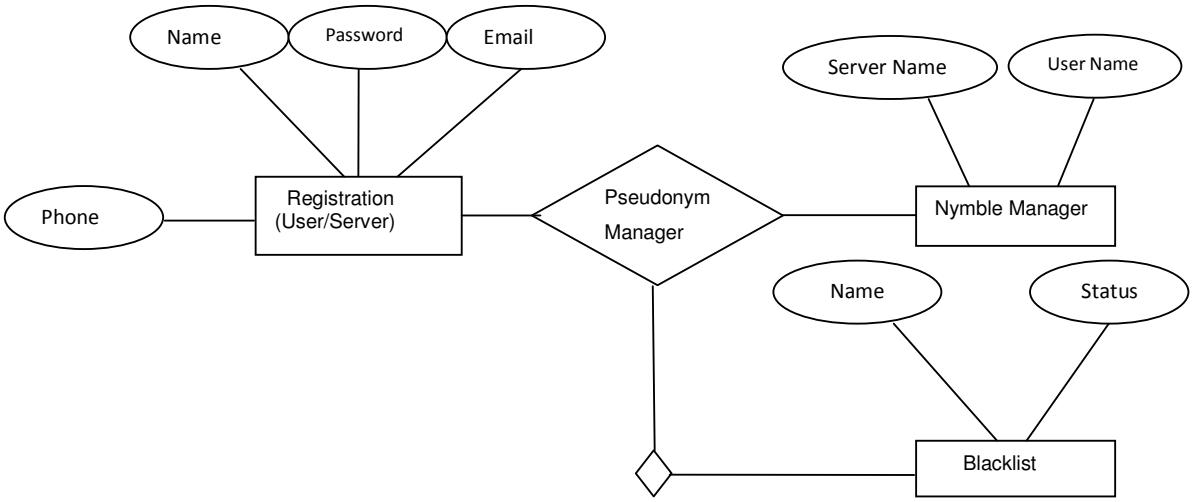
Output: Display complaints of user

III. ALGORITHAM USED

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 nymble appears in the server's blacklist.

Message authentication code (MAC)

Secure cryptographic hash functions. These are oneway and collision-resistant functions that resemble random oracles. Denote the range of the hash functions by H. Secure message authentication (MA). These consist of the key generation (MA.KeyGen), and the message authentication code (MAC) computation (MA.Mac) algorithms. Denote the domain of MACs by M. Secure symmetric-key encryption (Enc). These consist of the key generation (Enc.KeyGen), encryption (Enc.Encrypt), and decryption (Enc.Decrypt) algorithms. Denote the domain of ciphertexts.



Secure digital signatures (Sig) . These consist of the key generation (Sig.KeyGen), signing (Sig.Sign), and verification (Sig.Verify) algorithms. Denote the domain of signatures by

Algorithm 1. PMCreatePseudonym

Input: ðuid;wÞ 2 H_NN

Persistent state: pmState 2 SP

Output: pnym 2 P

1: Extract nymKeyP ; macKeyNP from pmState

2: nym :¼ MA:Macðuidkw;nymKeyP Þ

3: mac :¼ MA:Macðnymkw;macKeyNPÞ

4: return pnym :¼ ðnym; macÞ

Algorithm 2. NMVerifyPseudonym

Input: ðpnym;wÞ 2 P _NN

Persistent state: nmState 2 SN

Output: b 2 ftrue; falseg
1: Extract macKeyNP from nmState
2: ðnym; macÞ :¼ pnym
3: return mac ¼ ? MA:Macðnymkw;macKeyNP Þ

ANONYMIZING networks such as Tor 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 Web sites such as Wikipedia. Since Web site administrators cannot blacklist individual malicious users' IP addresses, they blacklist the entire anonymizing network.

IV. APPLICATION

- Our system ensures that users are aware of their blacklist status before they present a nymble, and disconnect immediately if they are blacklisted.
- In our system, the user can download the server's blacklist and verify her status. If blacklisted, the user disconnects immediately.

V.CONCLUDION

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 the 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.

5.1.FUTURE ENHANCEMENT

We hope that our work will increase the mainstream acceptance of anonym zing networks such as Tor, which has been completely blocked by several services because of users who bused their anonymity.

VI.REFERENCE

[1] G. Ateniese, J. Camenisch, M. Joye, and G. Tsudik, "A Practical and 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 Revocation in Group Signatures," Proc. Conf. Financial Cryptography, Springer, pp. 183-197, 2002.
[3] M. Bellare, R. Canetti, and H. Krawczyk, "Keying Hash Functions for Message Authentication," Proc. Ann. Int'l Cryptology Conf. (CRYPTO), Springer, pp. 1-15, 1996.
[4] M. Bellare, A. Desai, E. Jokipii, and P. Rogaway, "A Concrete Security Treatment of Symmetric Encryption," Proc. Ann. Symp. Foundations in Computer Science (FOCS), pp. 394-403, 1997.
[5] M. Bellare and P. Rogaway, "Random Oracles Are Practical: A Paradigm for Designing Efficient Protocols," Proc. First ACM Conf. Computer and Comm. Security, pp. 62-73, 1993.