National Conference on Advances in Computer Science and Applications with International Journal of Computer Applications (NCACSA 2012)
Proceedings published in International Journal of Computer Applications® (IJCA)

Blacklist based Anonymus User Blocking in IP Networks

Sruthi Franco
Final Year ME CSE Student
KCG College of Technology, Chennai

C Pradeesh Kumar
Assistant Professor
KCG College of Technology, Chennai

ABSTRACT

The framework to blacklist, track and block the anonymous user in IP network. The anonymous users are the users who are not valid or dishonest users. The IP network is network of computers using internet protocol for their communication. Anonymizing network is a type of IP network in which the identity of the user is hidden by using pseudonyms. The true identity of the user is not revealed i.e. the user remains anonymous. This anonymity is provided by using a series of routers to hide users' IP address. Some users misbehave in this network and they remain anonymous and the web server is not able to identify the real misbehaved users leading to the banning the anonymizing network. The misbehaved user is traced and blacklisted and again if they misbehave they are blocked by the web server. Therefore to block the misbehaving user and to give honest user anonymity, trusted third party is introduced. These help in blocking the misbehaving user preversing their anonymity. In this model the misbehavior can be defined by the web server. Therefore the anonymity and privacy of the blacklisted users are maintained even if they are banned from using the server again.

Keywords

IPNetwork,AnonoymizingNetwork,Anonymity,Blacklist,Privacy ,Pseudonym Manager,Blacklist Manager

1. INTRODUCTION

The base technology of internet does not require the users to identify themselves. The service providers usually enforce the identification of users for the purpose of billing and managing the abuse. The users communicate or execute web transactions in anonymizing network like Tor [18][21]. The user accesses the network and send request to the web server. This request is sent to web server through a random number of intermediate nodes. The user passes the request to a random node of anonymizing network. The request reaches the web server through a series of random intermediate nodes .Therefore the web server is unable to identify the true initiator. This is both an advantage as well as a disadvantage.

The disadvantage is that an honest user may be incorrectly suspected of originating the request and in some cases can even be banned from accessing the web server. The advantage is that the users' identity will not be revealed and they can express their views openly. The basic property of anonymous communication is sender anonymity, receiver anonymity and unlinkability of receiver and sender. The unlinkability of sender and receiver means that the path between the sender and receiver cannot be tracked or linked. Therefore it is not possible to find real sender and the receiver.

The anonymous communication means license to misbehave. In case of user misbehavior it is difficult to identify the real culprit, which is the main disadvantage of the anonymous communication. Due to the misbeviour the performance of the network will be degraded. Therefore the web server doesn't usually favour the anonymizing network. Therefore they tend to ban the user access through anonymizing network completely; even the honest users won't be able to access through these types of networks. It is necessary to block the misbehaving user and allowing only the honest users to access the anonymizing network. There are many methods to block the misbehaving users and also preserve their anonymity.

Pseudonym credential systems[10][14][28] allow the user to access the web pages using some pseudonyms and if misbehaved the users are blocked based on these pseudonyms. But in this all the users use pseudonyms, weakening the anonymity in the anonymizing network.

Group signature[1][2][7] scheme allow the group member to sign anonymously on behalf of the group .This provides anonymity to the signer. Its main application is in case of voting and bidding. But in case of conflict or misbehavior, group manager opens the group signature and identity of the user is revealed. But the server must query the group manager for every authentication lacking scalabilty.This method does not provide anonymity to the misbehaved users.

Traceable signatures [8][13][26] apply basic data mining technique where signature values of selective misbehaving users are traced. The user should be capable of claiming that he is the owner of the signature values. This leads to the self traceability property. But it does not provide backward unlinkability.Backward unlinkability means the user's accesses to the network before the complaint should remain anonymous.

Dynamic accumulators[11] are accumulators that allow one to dynamically add and delete input. The cost of adding and deleting is independent of the number of the accumulated values. It uses the RSA algorithm. It is an efficient membership revocation in the anonymous settings. Public parameters of the group must be checked and existing users' credential must always be updated which is impractical.

2. SYSTEM ARCHITECTURE

A system having properties like anonymous authentication, backward unlinkability, subjective blacklisting, fast authentication speeds, rate limited anonymous connections and revocation auditability is introduced. These properties can be implemented by introducing two trusted third parties namely Pseudonym Manager and Blacklist Manager.

The system architecture consists of user, service provider and trusted third parties the blacklist manager and the pseudonym manager.

If the user wants to execute web transaction, the user first registers with the Pseudonym Manager and issues user with pseudonym based on the IP address provided by it. The service provider registers with the Blacklist Manager which issues set of unique set of tokens.The user using its pseudonym name access the service provider through the anonymizing network. The service provider transfers the pseudonym to the Blacklist Manager. The Blacklist Manager consists of blacklist table. It has attributes like pseudonym, unique token, and blacklist value. Before the Service Provider give access, it checks with the

blacklist table, if the pseudonym is present in the blacklist table, then the user is denied access to SP, else the user can access freely through the network and the Service Provider.

All the connections of the user before the control was made will be unlinked i.e the accessing information of user can't be traced back. But after the complaint is made, were all the connections of the user will be linked. This above property helps in maintaining anonymity of the user, eventhough it is blacklisted.

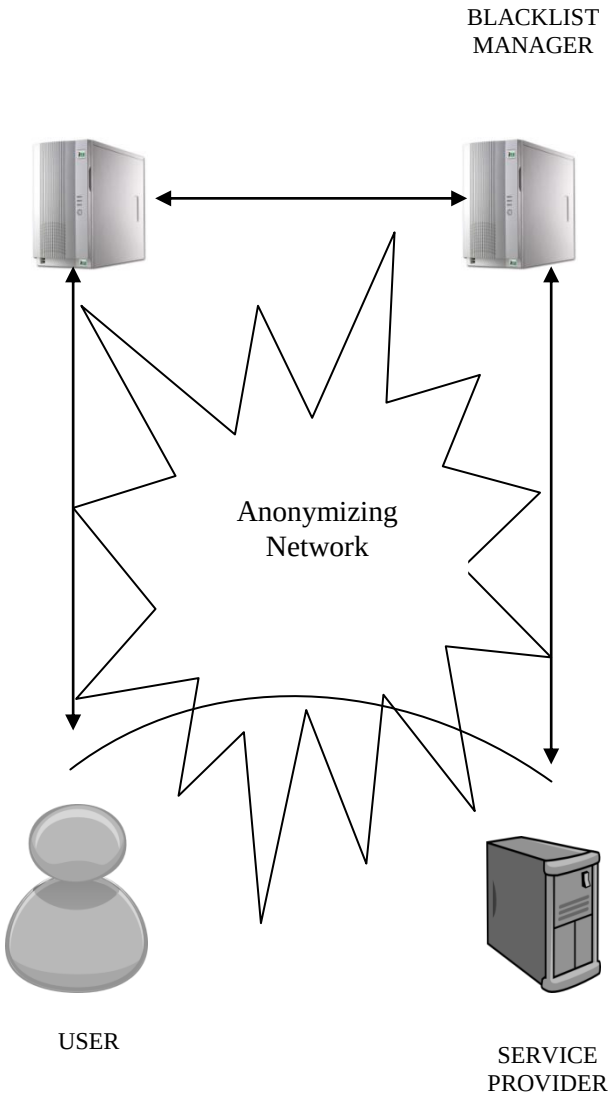

Fig1 System Architecture showing interaction between the nodes

3. IMETHODOLOGY

The main entities of this framework are the Pseudonym Manager, Blacklist Manager, user and the Service Provider. The Pseudonym Manager does the registration of new user, authentication and verification. The blacklist manager issues the unique tokens, maintains a blacklist table and link /unlink option based on whether the user access. The Service Provider registers with the blacklist manager which maintains a blacklist table.

A. Blacklist Manager and Pseudonym Manager

Blacklist manager controls the entire process of the whole architecture. Both the Service Provider and the Pseudonym Manager can be only accessed through the Blacklist Manager. It contains blacklist table which contains the attributes of pseudonym, tokens, blacklist status.

Pseudonym manager controls the user activities. Users can access the anonymizing network only if they register with the Pseudonym Manager. It has knowledge about the routers in the anonymizing network. Pseudonyms are chosen based on controlled resources such that no two users can have the same pseudonym. The user connections are anonymous to Pseudonym Manager. It is created to reduce the load from the Blacklist Manager. It also acts as second server to the system.

B. Time

Tokens generated by the blacklist manager are bound to specific time periods called the linkability window. This linkability window is again divided small time intervals. Users' access within a time period is tied to single token generated by the Blacklist Manager. The use of different tokens across time periods grants the user anonymity between time periods — smaller time periods provide users with higher rates of anonymous authentication, and likewise longer time periods rate-limit the number of misbehaviors from a particular user before he or she is blocked.

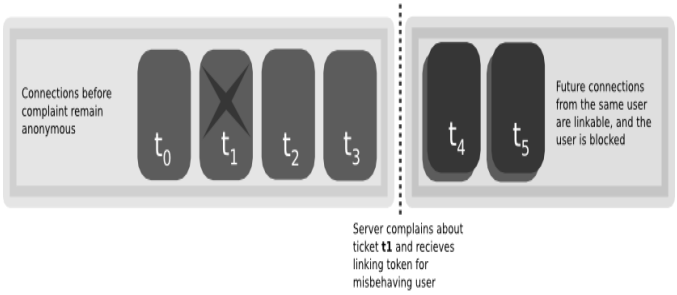

Fig2 Linkability Window

The linkabikity window has two purposes i.e. allows dynamism since resources like IP address can get reassigned among different users so that is difficult to blacklist the resource for long time and it ensures forgiveness for some time after being misbehaved.

C. Permission Control and Blacklist

All the user details are maintained both at Pseudonym Manager and the Blacklist Manager. Authorized and unblocked users can access the anonymizing network. Blocked user cant access the network, but with the permission of the Blacklist Manager it can access.

If the user misbehaves, service provider will link the future connections within current linkability window. Even though misbehaving user can be blocked from making any other connection, users past connection remain unlinkable.The service providers can subjectively judge users for any reason, since the privacy of users are maintained.

D. Notification of Blacklist Status

Users expect their connections to be anonymous while using the anonymizing network. In case of misbehavior of user, its future connection will be linked. Therefore the user should be able to view their blacklist status while trying to connect to the service provider. The user is able to download the blacklist table can check whether he is on the list. If present, user disconnects immediately.

E. User Details and User Access Control

All the user details and the access history will be maintained at database of both the pseudonym manager and the service provider. If the user misbehaves all those history will be updated to both the database.

4. SECURITY MODEL

This system provides four security goals. These goals help to resist the collision attacks.

Goals and Threats

The user is a honest user if it obeys the system specification. A honest user becomes corrupt when it infer the knowledge that he is denied of and makes compromise with the attacker. The corrupt users reveal all information and deviates from the system specification.

A. Blacklistability

It ensures that any honest user can block the misbehaving users. If an honest user complains about a misbehaving user in current linkability window then that user won't be able to reconnect.

B. Rate Limiting

No user can successfully connect to it more than once within single time period.

C .Anonymity

A legitimate user is the one who has not been blacklisted by the service provider and had not exceeded rate limit of reestablishment of connections. Anonymity protects the anonymity of all the users. The service provider just knows that the user is legitimate or not.

D. Non Frameability

Honest users who are legitimate can connect to the service provider preventing the attacker from framing the legitimate user.

5. ANALYSIS AND RESULT

Fig 3 shows size of the entities used in this framework. The x-axis shows the number of entries i.e the complaints in the blacklist update request, tokens generated by the blacklist manager, seeds in the blacklist update response. Assume L be the number of time periods in the linkability window. And credential is the collection of tokens.

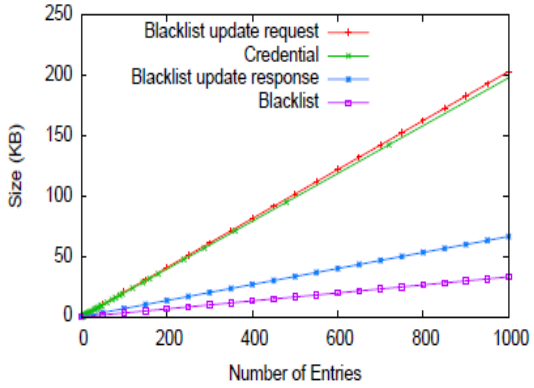

Fig 3 Size of entities Vs Number of entries

If linkablity window of one day is 5 minutes, then time period L=288.Each entity grows as number of entities grows. Credential and blacklist update request grows with the same rate because credential is same as complaint list sent when the blacklist table is to be updated.

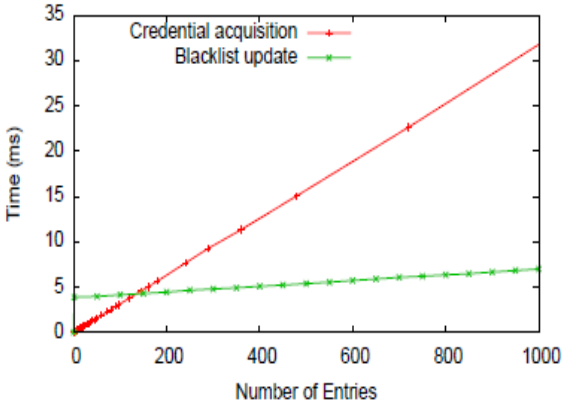

Fig 4 Performance Vs Number of entries

The above figure fig 4 shows the amount of time the blacklist manager takes to perform. Suppose it takes about 9ms to create a credential when L=288.Therefore a protocol that occurs only once every linkability window for each user wanting to connect to the service provider. For blacklist updates, the initial jump in the graph corresponds to the fixed overhead associated with updating the blacklist. If there is no complaint then it takes blacklist to less than millisecond for updating.

6. CONCLUSION AND FUTURE WORK

A framework is introduced in which helps in efficient and correct use of anonymizing network. Service provider can blacklist misbehaving users while maintaining their privacy and anonymity. This framework helps in practical, efficient and sensitive use of both user and service provider. This also increases the acceptance of anonymizing network which has been banned by different service providers due to misbehaving tendency of the users due to their anonymity. This is an application oriented software which simulates the blocking of misbehaving users in an anonymizing network. The resource used for generating pseudonym is the static IP address.

This model can be implemented in larger network. This framework can be extended so that service provider can find repeated misbehaving users and block users for longer period of time. Finding repeated users means , there should be a provision to link between different linkability window.

7. REFERENCES

[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 Revocationin Group Signatures," Proc. Conf. Financial Cryptography, Springer, pp. 183-197, 2002.

[3] M. Bellare, R. Canetti, and H. Krawczyk, "Keying Hash Functionsfor 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.

[6] M. Bellare, H. Shi, and C. Zhang, "Foundations of Group Signatures: The Case of Dynamic Groups," Proc.

Cryptographer's Track at RSA Conf. (CT-RSA), Springer, pp. 136-153, 2005.

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

[8] S. Brands, "Untraceable Off-Line Cash in Wallets with Observers(Extended Abstract)," Proc. Ann. Int'l Cryptology Conf. (CRYPTO),Springer, pp. 302-318, 1993.

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

[10] 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.

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

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

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

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

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

[16] C. Cornelius, A. Kapadia, P.P. Tsang, and S.W. Smith, "Nymble: Blocking Misbehaving Users in Anonymizing Networks," Technical Report TR2008-637, Dartmouth College, Computer Science, Dec. 2008.

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

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

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

[20] S. Even, O. Goldreich, and S. Micali, "On-Line/Off-Line Digital Schemes," Proc. Ann. Int'l Cryptology Conf. (CRYPTO), Springer, pp. 263-275, 1989.

[21] J. Feigenbaum, A. Johnson, and P.F. Syverson, "A Model of Onion Routing with Provable Anonymity," Proc. Conf. Financial Cryptography, Springer, pp. 57-71, 2007.

[22] S. Goldwasser, S. Micali, and R.L. Rivest, "A Digital SignatureScheme Secure Against Adaptive Chosen-Message Attacks," SIAM J. Computing, vol. 17, no. 2, pp. 281-308, 1988

[23] J.E. Holt and K.E. Seamons, "Nym: Practical Pseudonymity for Anonymous Networks," Internet Security Research Lab Technical Report 2006-4, Brigham Young Univ., June 2006.

[24] 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.

[25] A. Juels and J.G. Brainard, "Client Puzzles: A Cryptographic Countermeasure Against Connection Depletion Attacks," Proc. Network and Distributed System Security Symp. (NDSS), 1999.

[26] 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.

[27] B.N. Levine, C. Shields, and N.B. Margolin, "A Survey of Solutions to the Sybil Attack," Technical Report 2006-052, Univ. of Massachusetts, Oct. 2006.

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

[29] S. Micali, "NOVOMODO: Scalable Certificate Validation and Simplified PKI Management," Proc. First Ann. PKI Research Workshop, Apr. 2002.

[30] T. Nakanishi and N. Funabiki, "Verifier-Local Revocation Group Signature Schemes with Backward Unlinkability from Bilinear Maps," Proc. Int'l Conf. Theory and Application of Cryptology and Information Security (ASIACRYPT), Springer, pp. 533-548, 2005.