 ISSN : 0976-8491 (Online) | ISSN : 2229-4333 (Print)

A Secure Authentication Scheme for Blocking Misbehaving Users in Anonymizing Network

[1]Sathiya D, [2]Aravinthan K
[1,2]Dept. of CSE, SNS College of Engineering, Coimbatore, Tamil Nadu, India

Abstract
Some of the users start defacing the websites through anonymous network. Finding the misbehaving users in anonymizing network such as tor is not possible as they allow users to access internet services privately by using a series of routers to hide the client's IP address from the server. As a result, administrators block all known exit nodes of anonymizing networks, denying anonymous access to misbehaving and behaving users alike. To address this problem distributed nymble with client puzzle techniques are introduced in which honest users remain anonymous and their requests are unlinkable, a server can complain about a particular anonymous user and gain the ability to blacklist the user for future connections, this blacklisted user's accesses before the complaint remain anonymous and users are aware of their blacklist status before accessing a service and also the system is agnostic to different servers definitions of misbehavior. Scalability and robustness is achieved automatically as a result of the distributed system.

Keywords
Anonymizing Network, Client Puzzle, Defacing Users, Service Providers

I. Introduction

Anonymous authentication gives users access to the public areas of the Web or FTP site without prompting them for a user name or password. Some of the users start defacing the websites through anonymous network. Finding the misbehaving users in anonymizing network such as tor is not possible because the clients IP address is hidden from the servers. To address this problem several authentication schemes [1-4] are introduced. In these methods some use TTP's where others don't. The basic goal of these schemes are connecting the honest and trusted users anonymously and revoking the misbehaving users. Revoking is done with the help of the Revocation List. The users who are in Revocation List are no more anonymous. Authentication is designed that allow no one, not even an authority, identify users who have been authenticated within the allowable number, and also it allows anyone to trace, without help from the authority, dishonest users who have been authenticated beyond the allowable number by using the records of these authentications In pseudonymous credential systems [5] 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 [6-7], employ group signatures. Basic group signatures [8-9], 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.

To address the above problem, we present a secure system called Nymble, which provides all the following properties: anonymous authentication, backward unlinkability, subjective blacklisting, fast authentication speeds, rate-limited anonymous connections, and revocation auditability.In Distributed 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. Web sites, 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. Our system ensures that users are aware of their blacklist status before they present a nymble, and disconnect immediately if they are blacklisted.

II. Existing System

A. Blacklistable Anonymous Credentials

BLacklistable Anonymous Credential (BLAC) system [1] is the first cryptographic construction of an anonymous credential system that supports anonymous blacklisting and subjective judging without relying on TTPs. SPs maintain their own blacklists of misbehaving users without knowing the identity of the misbehaving users thus the blacklisted users remain anonymous. With anonymous credential system users can be blacklisted in a way that it preserves their anonymity, is based on subjective definitions of misbehavior and does not rely on a TTP. Deanonymizing a user is not always necessary to discourage misbehavior; in certain cases it is sufficient to simply block misbehaving users from making future accesses, while maintaining their anonymity. This property is called anonymous blacklisting. BLAC System can only blacklist the defacing users and cannot able to block them and they remain anonymous as well.

B. Privacy Enhanced Revocation with efficient Authentication (PEREA)

PEREA a new anonymous authentication scheme in which the computation is independent of the size of the revocation list and the time complexity of authentication is linear in the size ($K << L$) of a revocation window that is the number of subsequent authentications before which a user's misbehavior must be recognized if the user is to be revoked. Anonymous authentication schemes allow users to authenticate to service providers (SPs) as some anonymous member of a group. Fully-anonymous authentication, however, can give users the license to misbehave since they cannot be held culpable for their actions. For example, a website such as Wikipedia may allow anonymous postings, but then cannot hold users who deface webpage's accountable. To mitigate this problem, several schemes support revocation of anonymous users, where a Trusted Third Party (TTP) can take action against misbehaving users. At a high level, authentication in these schemes requires users to send SPs their pseudonyms encrypted with the TTP's key. SPs can present a misbehaving user's escrowed identity to the TTP as part of a complaint procedure. Advantages of this system is it eliminates TTPs is and an effective alternative and is rate limiting.

C. Nymble System

1. Resource-Based Blocking

To limit the number of identities a user can obtain the Nymble system binds nymbles to resources that are sufficiently difficult to obtain in great numbers. The following figure is the architecture of nymble:

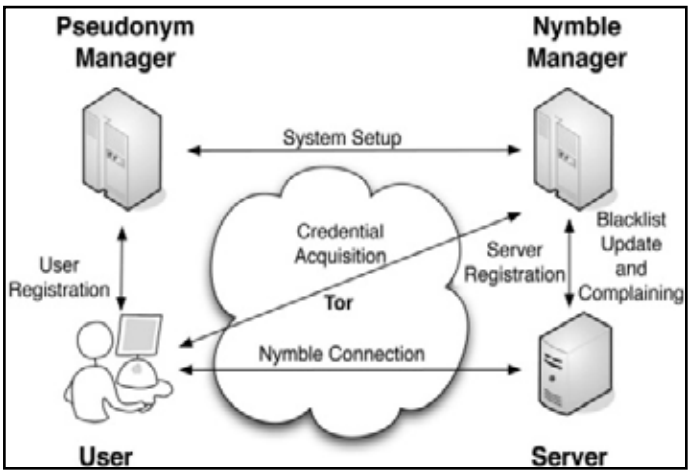

Fig. 1: Nymble System Architecture

2. The 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 fig. 1.

3. The 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. 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.

4. Blacklisting a User

If a user misbehaves, the server may link any future connection from this user within the current linkability window. If a user connects and misbehaves at a server during time period t* within linkability window w*. The server later detects this misbehavior and complains to the NM in time period tc ($t^* < tC < tL$) of the same linkability window w*. 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 user in time periods t_c; $t_c+1, \ldots, t_L$ of the same linkability window w* to the complaint. Therefore, once the server has complained about a user, that user is blacklisted for the rest of the day, for example (the linkability window). The user's connections in t_1; t_2; . . . ; t*; t*+1, . . . , t_c remain unlinkable (i.e., including those since the misbehavior and until the time of complaint). 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. The Blacklisted users are immediately updated in the Nymble manager and thus the users can see whether they are blacklisted or not.

This system has the drawbacks such as nymble managers are heavily loaded as it needs to authenticate the honest users and also has to register servers, blacklist the misbehaving users as well. Moreover there is a chance of nymble manager to fail because of DOS attack which leads to go entire system out of service. It did not support varying linkability window so we propose the system called distributed nymble which excludes pseudonym manager and includes nymble managers.

III. Proposed System

A. Distributed Nymble

In this system the series of nymbles are generated for connecting to the websites. These nymble cannot be shared and thus it is trusted.

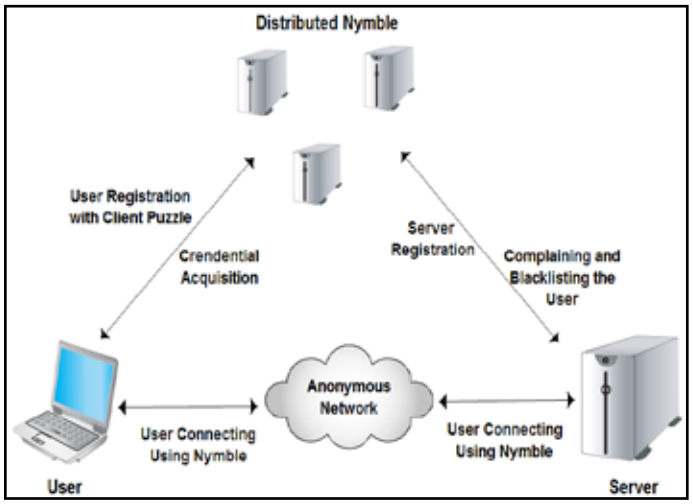

Fig. 2: Distributed Nymble Architecture

The User has to register with nymble before accessing to the server. Registration is done with the help of client puzzle techniques which is the first step in getting the nymbles from distributed nymble managers. Once the user acquires the nymbles they are ready to get access to the server through anonymizing network. Each server has to register with the nymble managers in order to agree that they will provide the service for the authenticated users. Later if the user misbehaves the servers can able to complain to the nymble managers and get their future nymbles to be linked whereas nymble which the user used before misbehaving remains anonymous. In the construction of the distributed Nymble system, initially an algorithm for server registration with the Nymble Manager is proposed. Next an algorithm for the User registration by client puzzle techniques is presented. Next a distributed Nymble connection to a server is established; here a user must provide a valid ticket, which is acquired as part of a credential from the Distributed NM. To acquire a credential for server sid during the current linkability window, a registered user initiates a type-Anon channel to the NM, followed by the Credential Acquisition protocol presented in this approach. Next a connection is established to a server sid, the user initiates a type-Anon channel to the server by the Nymble connection establishment protocol. 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. Next the approach for

blacklisting the user behind a Nymble connection is presented during the establishment of which the server collected ticket from the user; the server files a complaint by appending ticket to cmplnt-tickets in its svrState. Finally updates of the complaints will be takes place and a periodic updating is done. Performance evaluation implements Distributed Nymble manager and collected various empirical performance numbers, which verify the linear time and space costs of the various operations and data structures.

IV. Conclusion

In this system servers can blacklist misbehaving users while maintaining their privacy which also increases 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. The current system is further enhanced to show how the robustness of authentication protocols against denial of service attacks can be improved by asking the client to commit its computational resources to the protocol run before the server allocates its memory and processing time. The server sends to the client a puzzle whose solution requires a brute-force search for some bits of the inverse of a one-way hash function. The difficulty of the puzzle is parameterized according to the server load. The server stores the protocol state and computes expensive public-key operations only after it has verified the client's solution. The puzzles protect servers that authenticate their clients against resource exhaustion attacks during the first messages of the connection opening before the client has been reliably authenticated.

References

[1] P.P. Tsang, M.H. Au, A. Kapadia, 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.

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

[3] P.P. Tsang, M.H. Au, A. Kapadia, S.W. Smith,"PEREA: Towards Practical TTP-Free Revocation in Anonymous Authentication", Proc. ACM Conf. Computer and Comm. Security, pp. 333- 344, 2008.

[4] C. Cornelius, A. Kapadia, P.P. Tsang, S.W. Smith, 'Nymble: Blocking misbehaving users in anonymizing networks' Vol. 8, No. 2 pp. 256-269, 2011.

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

[6] J. Camenisch, 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.

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

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

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

SATHIYA D. received BE degree in computer science and Engineering from Anna University Coimbatore, Tamil Nadu, India in 2011.She is currently pursuing her M.E in Computer Science and Engineering from SNS College of engineering, Coimbatore .Her research interest include Cryptography and Network Security.

ARAVINDHAN K. received BE degree in computer science and engineering from Anna university Chennai in 2007 and ME degree in computer science and engineering from Kumaraguru College of Technology, Coimbatore in 2009. Presently he is working as Assistant Professor in Department of Computer Science and Engineering, SNS College of Engineering, Coimbatore, Tamil Nadu. His area of interest includes Wireless Sensor Network, VANET, and Network Security.