International Journal of Interdisciplinary Innovative Research &Development (IJIIRD)
ISSN: 2456-236X
Vol. **06** Special Issue **01** | **2021**

Review over Nymble Server

Anand A. Maha[1], Jayprakash D. Sonone[2], Ayaz M. Shaikh[3]

[1]Lecturer (Polytechnic), Department of Computer Science and Engineering, Padm. Dr. V. B. Kole Colege of Engineering, Malkapur, Maharashtra, India
[2]HOD (Polytechnic), Department of Electrical Engineering, Padm. Dr. V. B. Kole Colege of Engineering, Malkapur, Maharashtra, India
[3]Lecturer (Polytechnic), Department of Computer Science and Engineering, Padm. Dr. V. B. Kole Colege of Engineering, Malkapur, Maharashtra, India

ABSTRACT

The anonymizing network is network which hides the clients IP address from the server by using the sequence of the routers. But users are using this network for defacing the popular websites. Currently these popular website administrator blocks the IP address of the malicious user. But if user is inside the anonymizing network then website administrator will not able to find the IP address of the owner. Then the administrator will block all the existing nodes of the anonymizing network. This will deny the anonymous access to the misbehaving nodes along with users which are not misbehaving. To solve this problem we present the Nymble which will block only those users which are misbehaving inside the network. Also we are maintaining the privacy of those nodes which are behaving maliciously inside the anonymizing network.

Keywords: Onion routing, anonymous blacklisting, privacy, revocation

1. Introduction

Now a day many internet users don't want share their location and Identification for accessing the internet anonymously. Tor directs Internet traffic through a free, worldwide, volunteer network consisting of more than five thousand relays to conceal a user's location and usage from anyone conducting network surveillance or traffic analysis. Using Tor makes it more difficult for Internet activity to be traced back to the use. Tor's use is intended to protect the personal privacy of users, as well as their freedom and ability to conduct confidential communication by keeping their Internet activities from being monitored.

As we discuss above the TOR is able to hide the user's identity and the location from the others. So the TOR user can able to behave maliciously on any popular website like YouTube, Wikipedia. The existing system gives several solutions to this problem, Pseudonymous systems users log into websites using duplicate name called as pseudonyms, this pseudonym can be added to a blacklist if a user misbehaves on that site. But, this approach results in pseudonymity for all users, and it b locks the all user which are inside the anonymous network. The basic pseudonymous systems creates group of users in which all users can submit their complaint to the central manager. The server has to query to the group manager for each authentication. And due to which the scalability of the network get reduced. To track the particular user the group manger opens the trapdoor. Each server maintains the subjective blacklist in which all the misbehaving users are added. So that, the names of the blacklisted users are remain private.

Our system is several thousand times faster than VLR, which takes the server about one millisecond per authentication. We believe these low overheads will incentivize servers to adopt such a solution when weighed against the potential benefits of anonymous publishing. Data anonymization is the procedure of destroying the electronic trail or tracts, on the data that would show the way to an eavesdropper to its origins. Anonymizing networks for example Tor or I2P provides a strong way to anonymizing Internet communications, so that is will be very hard to link communication parties. There are several forms of credential systems evolved over the time in anonymizing networks. Anonymous communications networks facilitate to resolve the actual and important problem of permitting users to communicate privately over the Internet.

2. Literature Survey

Many existing services limit user abuses like posting spam or inappropriate comments by blocking IP addresses of abusers, or requiring users to prove ownership of a valid email address when creating a user account, which can then be disabled if the user misbehaves. While the academic literature does not consider such measures to be strong deterrents, they are nevertheless widely implemented as a tradeoff between the

needs of servers to limit abuse, and the reluctance of users to maintain cryptographically strong digital identities or provide sensitive identity information (like bank or government identifiers) just to post a blog comment or edit a Wikipedia article.

Nymble Introduction

Nym is an extremely simple way to allow pseudonymous access to Internet services via anonymizing networks like Tor, without losing the ability to limit vandalism using popular techniques such as blocking owners of offending IP or email addresses. Nym uses a very straightforward application of blind signatures to create a pseudonymity system with extremely low barriers to adoption. Clients use an entirely browser-based application to pseudonymously obtain a blinded token which can be anonymously exchanged for an ordinary TLS client certificate. Nym grew out of a discussion on the Tor email list about Wikipedia's practice of blocking Tor users from making changes to articles. Wikipedia blocks most Tor exit nodes due to abusers who had used Tor in the past to avoid IP- address based bans. Privacy protecting credential systems were mentioned, but it was pointed out that such systems tend to be patent-encumbered and difficult to implement. Another problem was the basis for pseudonymity; privacy protecting credential systems are generally described in terms of large, established agencies issuing digital credentials to the masses. Such systems would create a high-stakes game of cryptographically certified personal information which would naturally tend to intimidate users of an anonymity network like Tor [3].

Credential System

A credential system is a system in which users can obtain credentials from organizations and reveal possession of these credentials. This system is called anonymous when transactions carried out by the same user cannot be linked. Anonymous credential system consists of users nothing but clients and respective organizations. These organizations know the users only by their pseudonyms. The basic system contains protocols. These protocols are used by user to join the system, and then to register with an organization and after that, obtain multiple show credentials, and show such credentials.

PEREA

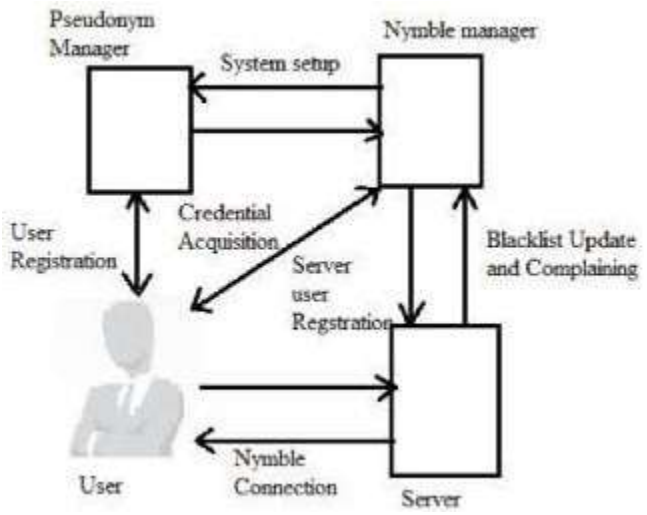
PEREA (Privacy-Enhanced Revocation with Efficient Authentication), an anonymous authentication scheme without TTPs in which the time complexity of authentication at the SP (the bottleneck operation) is independent of the size of the blacklist. Instead, the amount of computation is linear in the size K of the revocation window, the number of authentications before which a misbehavior must be recognized and blacklisted for a user to be revoked.

The Onion Routing

An onion-routing network consists of a set of onion routers and clients. To send data, a client chooses a sequence of routers, called a circuit, and constructs the circuit using the routers' public keys. During construction, a shared symmetric key is agreed upon with each router. Before sending data, these keys are used to encrypt each packet once for each router in the circuit and in the reverse of the order that the routers appear in the circuit. Each router uses its shared key to decrypt the data as it is sent down the circuit so it is fully decrypted at the end. Data flowing up to the client has a layer of encryption added by each onion router, all of which are removed by the client. The layered encryption helps hide the data contents and destination from all but the last router and the source from all but the first router. The multiple encryption and decryption also makes it harder for an observer to follow the path the data takes through the network.

3. Problem Statement

The Nymble, provides the properties like: backward unlinkability, anonymous authentication, fast authentication speeds, subjective blacklisting, rate-limited anonymous connections. Very firstly the user is connected to our Nymble system. Then Nymble generate a pseudonym to the user through which the user can connect to the website. Generally the particular website blocks the user by obtaining seed of a Nymble. Then in future when that particular user tries to access the website then by examining the Nymble of user the website can able to block the user without knowing its IP address and other additional information. If any user get blacklisted then Nymble immediately disconnect that user. Any number of users can be accessible through the single Nymble system.



The Fig-1 shows the system flow of the Nymble System. Which consist of 4 main modules.
These are
1. User,
2. Pseudonym Manager,
3. Nymble Manager,
4. Destination Server.

4. The Nymble Sever

a. Approach of Sybil Attacks

If any user in the network shows multiple identities to attack on system then that attack is called as Sybil attack. Now in Nymble system we are using the IP address, but in general it may be any data like email id. Here we are not going to solve the Sybil attack; we are only describing some mechanisms related to Sybil attack, as we are implementing this system as a real word application [8].

b. Traceable Signatures

Traceable signatures allow the group manager to release a trapdoor that allows all signatures generated by a particular user to be traced. This approach does not provide the backward unlinkability that they desire, where a user's accesses before the complaint remain anonymous. Backward unlinkability permits subjective blacklisting, where servers can blacklist users for whatever reason since the privacy of the blacklisted user is not at risk. In contrast, those approaches which are without backward unlinkability requires paying watchful attention to when, why a user must have all their connections linked. Users must concern about whether their behaviors will be judged fairly or not. Subjective blacklisting is suitable to the servers like Wikipedia where misbehaviors like questionable edits to a Webpage are difficult to define in mathematical terms. In some systems it is possible to define misbehavior accurately [5].

c. Managing the Pseudonyms

The user is initially connected to the Pseudonym manager (PM) before it going to use the resources. The pseudonym manager gives the pseudonym to user. After that PM prepares the pseudonym-Resource pair for particular user. Here the PM does not have any concern about the website on which the user wants to connect. It only stores the IP information about user resources.

d. Nymble Manager

After getting the pseudonym from the PM the user connects to the Nymble server. Then by using the pseudonym user can get access of the website trough the anonymous network. The Nymble system creates a pseudonym-server pair. Then it encapsulates that Nymble inside the Nymble Tickets. This will provide the cryptographic approach for better security. These tickets are concatenated with a time period. Less time periods provides high speed authentication to the user. The user will be authenticated only once for day.

e. Blacklisting User's

If the user misbehaves inside the network then it is consider as a malicious user and it is added to the Blacklist.

The server attaches the complaint link to the user resources and sends it to the NM. The NM returns Nymble ticket to the server along with seed. Once the user gets blocked then it is unable to reconnect for a day.

f. Analysis

Here we have used the IP Address for blocking the user. Due to which we can achieve both Nymble blocking as well as the IP blocking. A credential of the nymble system contains all the nymble tickets which are use for a particular linkability window that represents that a user can present at a particular server. The blacklist is nothing but a list of collection of nymble's which corresponds to all the complaining nymble. Users can easily check their blacklisting status at a server by checking their nymble inside the blacklist.

5. Conclusion

In this paper we are using the Nymble system to prevent misuse of anonymity. Our system maintains anonymity of users in anonymizing network which is remains essential. In practical the Nymble system is efficient system, and this can be used to add a extra layer of security to any publicly known more popular anonymizing network where servers can able to blacklist misbehaving users and can maintain their privacy.

References

[1] Patrick P. Tsang, Apu Kapadia, Member, IEEE, Cory Cornelius, and Sean W. Smith "Nymble: Blocking Misbehaving Users in Anonymizing Networks" Digital Object Indentifier 10.1109/TDSC. IEEE 2009..

[2] S. Goldwasser, S. Micali, and R. L. Rivest. A Digital Signature Scheme Secure Against Adaptive Chosen- Message Attacks. SIAM J. Comput., 17(2):281–308, 1988.

[3] 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.

[4] P. C. Johnson, A. Kapadia, P. P. Tsang, and S. W. Smith. Nymble: Anonymous IP-Address Blocking. In Privacy Enhancing Technologies, LNCS 4776, pages 113–133. Springer, 2007.

[5] Kiayias, Y. Tsiounis, and M. Yung, "Traceable Signatures," Proc. Int'l Conf. Theory and Application of Cryptographic Techniques (EUROCRYPT), Springer, pp. 571-589, 2004.

[6] Kiayias, Y. Tsiounis, and M. Yung. Traceable Signatures. In EUROCRYPT, LNCS 3027, pages 571–589. Springer, 2004.

[7] N. Levine, C. Shields, and N. B. Margolin. A Survey of Solutions to the Sybil Attack. Technical Report Tech report 2006- 052, University of Massachusetts Amherst, Oct 2006.

[8] Lysyanskaya, R. L. Rivest, A. Sahai, and S. Wolf. Pseudonym Systems. In Selected Areas in Cryptography, LNCS 1758, pages 184– 199. Springer, 1999.

[9] S. Micali. NOVOMODO: Scalable Certificate Validation and Simplified PKI Management. In 1st Annual PKI Research Workshop - Proceeding, April 2002.

Authors Profile

Prof. Anand A. Maha has completed his Master of Engineering from University of Pune. He is having teaching experience of 5 years and currently working as lecturer at Padmashri Dr. V. B. Klote COE, Malkapur. His area of interest is Dig Data, Network Security and IOT.

Prof. Jayprakash D. Sonone has completed his Master of Engineering from North Maharashtra University Jalgaon. He is having industrial experience of 8 years along with teaching experience of 10 years and currently working as HOD at Padmashri Dr. V. B. Klote COE, Malkapur. His area of interest is Electrical Power Generation, Power Electronics.

Prof. Ayaz M. Shaikh has completed his Master of Engineering from Sant Gadge Baba Amravati University. He is having teaching experience of 6 years and currently working as lecturer at Padmashri Dr. V. B. Klote COE, Malkapur. His area of interest is programming in C and C++, Cyber security.