ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 4, Issue 7, July 2015

Nymble Credential System (Blacklisting Misbehaving Users in Anonymizing Networks)

Shani J S

Asst. Professor, Dept. of Computer Science, L B S Institute of Technology for Women,

Poojappura, Trivandrum, Kerala

Abstract: 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 websites. Website administrators routinely rely on IP-address blocking for disabling access to misbehaving users, but blocking IP address is not practical if the user 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. To address this problem, a solution is to be implemented is called Nymble Credential System, a system in which servers can blacklist misbehaving users, thereby blocking users without compromising their anonymity. This system is agnostic to different servers' definitions of misbehaviour- servers can blacklist users for whatever reason, and the privacy of blacklisted users is maintained.

Keywords: Privacy, Anonymity, blacklisting, misbehaving, linkability window.

I. INTRODUCTION

The internet is computer based global information system. It is composed of many interconnected computer networks. Each network may link thousands of computers enabling them to share information. The internet has brought a transformation in many aspects of life. It is one of the biggest contributors in making the world into a global village. Use of internet has grown tremendously since it was introduced. It is mostly because of its flexibility.

Everyone's daily life, People access to Internet to do business, to find job, to contact friends, to pay bills. With the impact of Internet on society, people became more sensitive regarding privacy issues in the Internet. They realized that they leave all kinds of traces and personal information while surfing websites and exchanging emails. In some cases, people do not want others know what they are talking. While end-to-end encryption can protect the data content of communications from adversarial access, eavesdropping on content becoming very difficult. However, preserving privacy means not only the content of messages, but also hiding routing information which means who is talking to whom. One well known solution to keep privacy involves issuing the queries via an anonymizing network, such as Tor.

A. Problem Definition

In anonymizing network, the identity of the user is hidden from search engine by using pseudonyms. The true identity of the user is not revealed i.e.; the user remains anonymous. This anonymity allows users to access Internet services privately by using a series of routers to hide the client's IP address from the server. Through this anonymous property, people are more equal in discussions, factors like status, gender, etc., will not influence the evaluation of what they say. They can openly discuss the personal stuff without revealing their real identity.

Unfortunately, some users have misused such networks under the cover of anonymity; users have repeatedly defaced popular Web sites. Since web site 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. 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, misbehaviour can indeed be defined precisely. For instance, double spending of an e-coin is considered misbehaviour in anonymous e-cash systems.

To address these problems, the solution is to be implemented is called Nymble Credential System, a system in which servers can "blacklist" misbehaving users, thereby blocking users without compromising their anonymity. In this system, servers can blacklist users for whatever reason, and the privacy of blacklisted users is also maintained.

II. SYSTEM OVERVIEW

The proposed system provides servers with a means to block misbehaving users of an Anonymizing network. The Nymble System consists of four actors namely the pseudonym manager, the Nymble Manager, user and the server. This system enables the service providers such as the websites to offer anonymous access to the services while allowing them to blacklist anonymous users who have misbehaved. Websites can block users by obtaining a seed for a specific nymble, and thus allowing them to establish a connection with future nymbles from the user

ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 4, Issue 7, July 2015

— and those prior to the complaint remain unlinkable and untraceable. Servers can thus block anonymous users without gaining access to their IP addresses while allowing legitimate users to connect anonymously.

This system let the users know about their blacklisted status before they are introduced to a nymble, and are disconnected immediately in case they are blacklisted. A large number of anonymizing networks can rely on the same Nymble system, and blacklisting anonymous users regardless of their anonymizing network. This blacklisting status affects only the future accesses, but the blacklisted anonymous users' previous activities remain anonymous and unlinkable. All blacklists expire at the end of system web administrator defined it as unlinkability window. Within a time period subdivision of the linkability window, the users activities are linkable and time period limit the rate of anonymous connections by users.

The modules of this system and their descriptions are listed below.

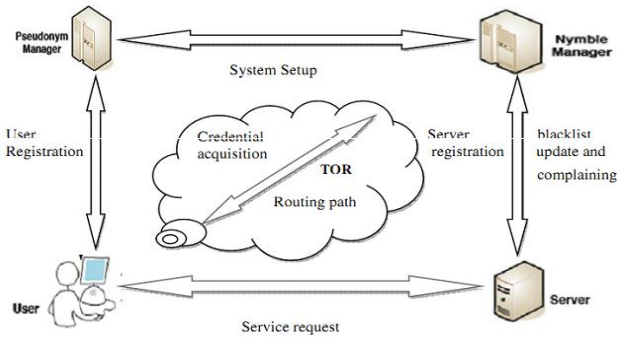

Fig. 2 Nymble System Architecture.

A. The Pseudonym manager

The user must connect to the Pseudonym Manager (PM) directly. The user first register with Pseudonym Manager to acquire the pseudonym. The user connects to the Pseudonym Manager directly not through any routing path. This enables the PM to identify the clients IP address. The work of PM is to generate a pseudorandom number. Thus the PM is responsible for identifying the user's IP address and generates a unique random number based on the user's IP address and physical address. But the PM is unaware of the service provider to whom the user wants to communicate.

B. The Nymble Manager

Post gaining a pseudonym from the PM, the user connects to the Nymble Manager via the anonymizing network, and then request for Nymbles to obtain 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. Nymbles are thus specific to a particular user-server pair. As long as the PM and the NM do not collude, the NM knows only the pseudonym-server pair, and the PM knows only the user identity-pseudonym pair. In order to provide the required cryptographic protection and security properties, nymbles are encapsulated within nymble tickets. Servers pack seeds into linking tokens, and therefore, linking tokens being used to link future nymble tickets. With the help of this linking token, the server can allow the users to proceed with the website or if blacklisted means it disconnect them.

C. Blacklisting a User

The server can present a user's nymble ticket to the Nymble Manager as a part of complaint. The Nymble Manager extracts a "linking token" from the nymble ticket, which will allow the server to link future connections by the blacklisted users. When the users defaces a website means the server then complaints to the Nymble manager providing the misbehaving user's nimble ticket. The Nymble Manager provides the server a linking token for the misbehaving users' nymble ticket. The server then adds the misbehaving users to the blacklist and the user is disconnected from the current linkability window of that website.

D. Notifying the user of blacklist status

Users using anonymizing networks want their connections to be anonymous. When a server obtains a seed for that user, it can still link the user's subsequent connections. It is very important that users be notified of being blacklisted before presenting a nymble ticket to a server. The user can thus download the server's blacklist and verify its status. When blacklisted, the user immediately gets disconnected.

E. System Setup

The system setup defines the interaction between the Pseudonym Manager and the Nymble Manager. The PM generates the unique pseudorandom number. Since PM knows only the client's IP address, but not the server which the client intend to access. The Nymble Manager knows the client's pseudonym assigned by the PM, but doesn't know the client's IP address. But the NM knows the server to which the client wants to access, because it needs to issue the client with a credential to access these sites. The PM and NM interacts directly with each other where they perform the resource matching mechanism. . Nymble manager uses MAC to verify the integrity of the pseudonym.

F. User Registration

A user with identity must register with the Pseudonym once each linkability window. The user, on receiving pseudonym, sets the state, and terminates with success.

G. Server Registration

A server with identity must register with the Nymble manager. Each server may register at most once in any likability window. The Nymble Manager makes sure that the server has not already registered.

H. Credential Acquisition

In order to establish an authenticated connection to a server, a user must provide a valid nymble ticket, which is acquired as a part of credential from the Nymble Manager. Since the system name itself ensures credential system it

ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 4, Issue 7, July 2015

mainly provides credential accessibility to the user to connect to the website. The credential offered to the client is nothing but a set of nymble tickets issued by the Nymble Manager in order to access the website.

I. Authenticated Connection

An authenticated connection is established successfully if the users' pseudonym gets matched with the Nymble Manager. The resource matching mechanism is done here by the Nymble manager, since the Pseudonym Manager and Nymble Manager interacts with each other. When a user presents his/her Nymble ticket to the server within the time period of the linkability window means the server identifies the user as a genuine user. But if the user defaces a website means the server complaints to the Nymble Manager along with the users' nymble ticket. Then the Nymble manager extracts a linking token to the server and blacklists the user. In such cases, servers disconnect the misbehaved users' connection from the current linkability window and deny their future access from their site.

J. Complaining and Blacklist Updates

In this system blacklist is kept up to date which contain nymble tickets of recent complaints and to be verified by the users in a time period during a linkability window. The server must update its blacklist by the first connection establishment request in each time period. If there is no complaints means then the server with the help of the linking token produced by the Nymble manager must establish the successful authentication connection. The complaints of the server are sent to the Nymble Manager. Since the Nymble Manager monitors the activities it stores the users' actions in the log file and update the blacklist status each and every time.

The proposed system aims the following security goals:
Anonymous blacklisting server can block the IP address of a misbehaving user without knowing the identity of the user.
Privacy: Honest and misbehaving users both remain anonymous.
Backward anonymity: The blacklisted user's previous activity remains anonymous and is refused future connections
Blacklist-status awareness: A user can check whether he has been blocked before accessing services at the server.
Subjective blacklisting: servers can provide their own defintions of misbehaviour
All **blacklists expire** at the end of system administrator defined it as unlinkability window.
Rate-limiting: ensures that no users can successfully connect it to more than once within any single time period.
Revocability: where users can verify whether they have been blacklisted.

III. CONCLUSION

This paper presented a secured credential system called the Nymble Credential System, which enables the service providers to blacklist the misbehaving users. Using this system, websites can blacklist users without knowing their IP addresses. When the users deface a website, the server then adds the misbehaving users to the blacklist and the user is disconnected from the current linkability window of that website. Furthermore, blacklisted users' previous connections remain anonymous. Since websites are free to blacklist anonymous users of their choice, and since users are notified of their blacklisting status, this system avoids the complications associated with judging "misbehavior." I believe that these properties will enhance the acceptability of anonymizing networks such as Tor by enabling websites to selectively block certain users instead of blocking the entire network, all while allowing the remaining (honest) users to stay anonymous.

REFERENCES

[1] Patrick P. Tsang, Apu Kapadia,Member, IEEE, Cory Cornelius, and Sean W. Smith, "Nymble: Blocking Misbehaving Users in Anonymizing Networks," IEEE Transactions On Dependable And Secure Computing, VOL. 8, NO. 2 ,2011

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

[3] [3] Zi Lin & Nicholas Hopper Computer Science & Engineering, "Jack: Scalable Accumulator-based Nymble System".

[4] [4] G. Ateniese, D.X. Song, and G. Tsudik, "Quasi-Efficient Revocation in Group Signatures," Proc. Conf. Financial Cryptography, Springer, pp. 183-197, (2002).

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

[6] [6] D. Boneh and H. Shacham, "Group Signatures with Verifier-Local Revocation," Proc. ACM Conf. Computer and Comm. Security, pp. 168-177, (2004).