International Journal of Modern Engineering Research (IJMER)
www.ijmer.com Vol. 3, Issue. 4, Jul. - Aug. 2013 pp-2320-2323 ISSN: 2249-6645

A Novel Method for Blocking Misbehaving Users over Anonymizing Networks

A. N. Venkata Krishna Gopichand[1], Syed Gulam Gouse[2]
[1]*M. Tech, Nimra College of Engineering & Technology, Vijayawada, A.P., India.*
[2]*Professor, Dept.of CSE, Nimra College of Engineering & Technology, Vijayawada, A.P., India*

ABSTRACT: *Nymble is a system that allows websites to selectively blacklist the users of anonymizing networks such as Tor without knowing the user's IP-address. Users not on the blacklist enjoy anonymity while the blacklisted users are not allowed future connections for a duration of time while their previous connections remain unlinkable. Nymble is based on two administratively separate "manager" servers, called the Pseudonym Manager (PM) and the Nymble Manager (NM). The PM is responsible for pairing a user's IP address with the pseudonym deterministically generated based on the user's IP address. The NM pairs a the user's pseudonym with the target server. The major problem is that the security of this system greatly depends on the assumption that the involved participants are honest and they are not going to collude to identify a user and link his connections. Another problem is that this system is neither scalable nor robust since there is only one Nymble Manager (NM) that has to be involved in the nymble ticket generation and complaining mechanisms. This paper presents a novel method for constructing a dynamic nymble system for solving the problems in original nymble system.*

KEYWORDS: *Anonymizing network, Nymble, Pseudonym.*

I. INTRODUCTION

Anonymizing networks such as Tor[1][2] route traffic through independent nodes in separate administrative domains to hide the client's IP address. Unfortunately, some users have misused such networks—under the cover of the 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 whole anonymizing network. Such measures eliminate the malicious activity through anonymizing networks at the cost of denying anonymous access to behaving users. Anonymizing networks such as Tor are widely deployed to preserve the privacy of the users while they access a service provided by a web server. These networks constitute an important class of a Privacy Enhancing Technology. However, some servers simply deny requests of users who connect through the anonymizing network since they don't have any protocol to punish misbehaving users.

Nymble[3] is basically a system that intends to bind the identity of an anonymous user to a pseudonym[4][5], generated from user's IP address using a one-way function, and simulates a service request with a ticket acquisition. This idea enables a server to complain about the misbehaviour of a user and blacklist his future tickets. Using this system honest users remain anonymous, a server can blacklist the future connections of particular users. Moreover, all the connections of a blacklisted user before the complaint remain anonymous and finally a user can check whether he is blacklisted or not at the beginning of a connection.

Nymble offers the following properties:

- **Anonymous blacklisting:** A server can block the Internet protocol (IP) address of a misbehaving user without knowing the identity of the user or his/her IP address.
- **Privacy:** Honest and misbehaving users both remain anonymous, which provides privacy.
- **Backward anonymity:** The blacklisted user's previous activity remains anonymous or unlinkable, and is refused future connections.
- **Blacklist-status awareness:** A user can check whether he/she has been blocked before accessing the services at the server.
- **Subjective judging:** Since misbehaving users are blocked without compromising their privacy, the servers can provide their own definition of "misbehavior".

II. EXISTING SYSTEM

Nymble is based on two administratively separate "manager" servers, called the Pseudonym Manager (PM) and the Nymble Manager (NM). The PM is responsible for pairing a user's IP address with the pseudonym deterministically generated based on the user's IP address. The NM pairs a the user's pseudonym with the target server. As long as the two managers are not colluding with each other, the user's connections remain anonymous to the PM, pseudonymous to the NM (note that the user does not communicate directly with the NM, and connects to the NM through Tor), and anonymous to servers that the user connects to. The user (in this case, Alice) must first demonstrate the control over a resource, that is the Alice's IP-address. To do this Alice must first connect directly with the PM before receiving the pseudonym. The PM has knowledge of existing the Tor routers, and thus can ensure that Alice is communicating with it directly. Note that the PM has no knowledge of the user's destination, similar to the entry node in Tor network. The PM's sole responsibility it to map IP addresses to the pseudonyms. Alice then connects to the NM through Tor network presenting her pseudonym and her target server. The NM does not know that the IP address of the user, but the pseudonym provided by the PM guarantees that some unique IP address maps to the pseudonym. She receives a set of "nymble" tickets as her credential for the target server.

These nymble tickets are unlinkable, and therefore Alice can present them nymble tickets (once each) to gain anonymous access at the target server. Figure 1 shows how a user connects to a server.

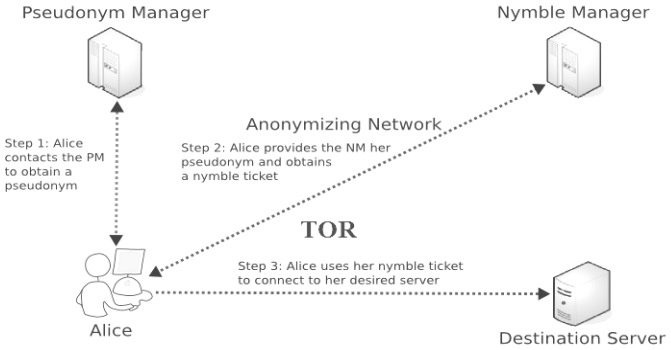

Figure 1: Connecting to a server

Servers can present the user's nymble ticket to the NM as part of a complaint. The NM extracts the linking token from the nymble ticket, that will allow the server to link future connections by the blacklisted user. The NM also issues the servers with blacklists, which the users can examine before performing any actions at the server. By checking servers' blacklists, the blacklisted users are assured that their privacy is not compromised. We now explain the process of blacklisting in a little more detail- nymble tickets are bound to certain "time periods" and "linkability windows.". Figure 2 shows the process of blacklisting a user.

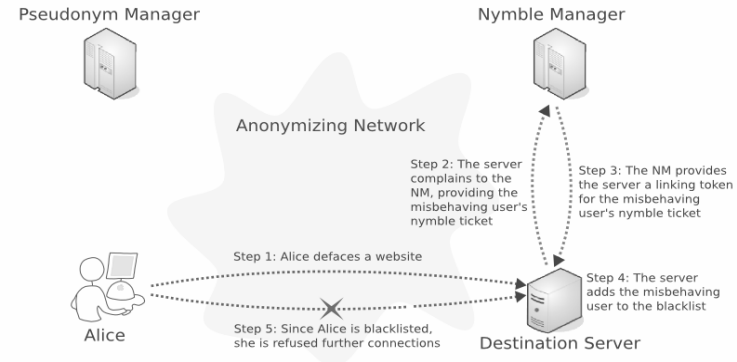

Figure 2: Blacklisting a user

The major problem is that the security of this system greatly depends on the assumption that the involved participants are honest and they are not going to collude to identify a user and link his connections. Another problem is that this system is neither scalable nor robust since there is only one Nymble Manager (NM) that has to be involved in the nymble ticket generation and complaining mechanisms.

III. PROPOSED SYSTEM

In the existing system, Pseudonym Manager (PM) is mapping IP addresses to pseudonyms. The pair (IP, pnym) is of more of real security concern. Here, one more layer of security is needed to add to that pair. In our proposed work (Figure 3), to do that, it requires some changes in the design of PM. The new pseudonym protocol needs two rounds of communication between the user and the set of Pseudonym Managers: In the first round, the user must choose a random PM and connect to it directly to request the codename, which is a pseudonym of his IP address. A request is valid if the user IP address does not come from a known anonymzing network and it has not been used before obtaining a codename in this likability window. The user chooses another random PM in the second round of the pseudonym registration. The user connects to that PM using an anonymizing network and sends her (codename,σ) pair to him. After obtaining the pair and verifying the ring signature [6], the PM issues a pseudonym, that the user can use it to connect to the Nymble Managers.

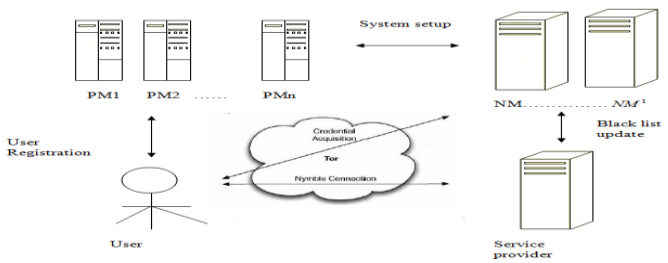

Figure 3: Pseudonym Construction

In the design of Nymble system, the Nymble Manager is an entity that is involved in ticket generation, linking token extraction and blacklist refreshment. Therefore, it might be heavily loaded if the system has many anonymous users and service providers. On the other hand, if Nymble Manager goes out of service for any reason like a a DoS attack or system failure, new users cannot subscribe into the system and service providers cannot extract linking token of misbehaving users. So we need more than one nymble manager. In this design every Nymble Manager should be able to do the following:

- Generate a chain of nymble tickets for the user
- Verify integrity of the nymble ticket without knowing the identity of its issuer
- Extract a linking token from the nymble ticket possibly issued by another Nymble Manager
- Guarantee freshness of the server's blacklist

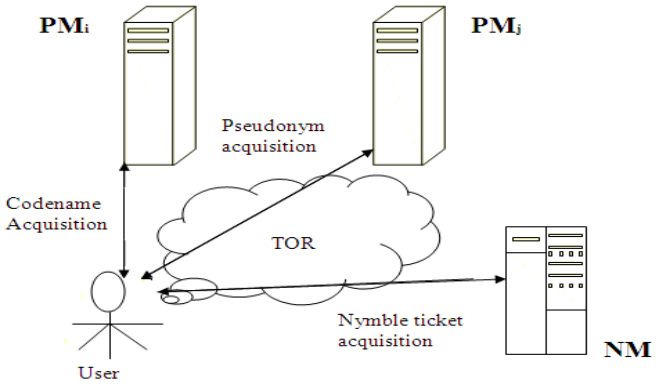

Figure 4: Integrity verification of Pseudonym by NM

The tasks of NM are: Nymble manager should first verify integrity of pseudonym and then generate nymble tickets for that connection (Figure 4). The NM should first verify the integrity of the nymble ticket and then decrypt it to obtain the linking token (Figure 5).

The Nymble Manager first runs NMVerifyPseudonym to check whether the pseudonym is valid or invalid. Then it runs NMCreateCredential to create the list of nymble tickets(called *creds*) for the user and sign every ticket using a ring signature scheme that allows other NMs and all servers to verify it. Algorithm 1 is used to verify the pseudonym by NM.

Algorithm 1: NMVerifyPseudonym
Input: {pnym,w}
Output: {true or false}
1 Extract verifyKeyPM1…n from keys in nmState
2 (nym,σnym) := pnym
3 return σnym == RingSig:Verify(nym|| || w, verifyKeyPM1…n)

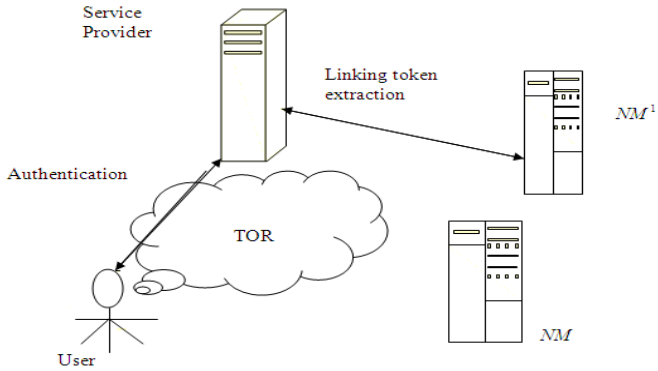

Figure 5: Integrity verification of Nymble ticket by NM

The Nymble manager verifies the nymble ticket by using algorithm 2.

Algorithm 2: NMVerifyTicket
Input: {sid,t,w,ticket}
Output: {true or false}
1 Extract verifyKeyNM1, NM2, NM3…NMm from keys in nmState
2 (nymblet,ctxt, σ_{ticket}) := ticket
3 return RingSig:Verify(sid||t||w|| $nymble_t$ ||ctxt, σ_{ticket} , verifyKeyNM1, NM2, NM3…NMm)

The Nymble Manager should also verifies the integrity of blacklist by running algorithm 3.

Algorithm 3: NMVerifyBL
Input: {sid, t, w, blist, cert}
Output: {true or false}
1 Extract verifyKeyNM1…m from keys in nmState
2 (td,daisy,ts, σ_{BL}) := cert
3 if td $\neq$t v td < ts then
4 return false
5 target := h(td−ts)(daisy)
6 return RingSig.Verify(sid||ts||w||target||blist, σ_{BL} ;
verifyKeyNM1…m)

IV. CONCLUSION

Nymble is a system which provides a blocking mechanism to a server to protect it from various misbehaving users without de- anonymization while allowing anonymous access to behaving users. But, the earlier design for Nymble had a disadvantage. The original design was based on an unrealistic assumption that the trusted third parties(TTP), Pseudonym Manager and Nymble Manage are not going to collude to identify the user. To eliminate this one, we propose a distributed nymble system. Our distributed architecture is not only scalable and robust, but it is more efficient than TTP free anonymous blacklisting systems like BLAC and PEREA.

REFERENCES

[1]. R. Dingledine, N. Mathewson, and P. Syverson, "Tor: The Second- Generation Onion Router," Proc. Usenix Security Symp., pp. 303- 320, Aug. 2004.
[2]. http://www.torproject.org.in/
[3]. Patrick P.Tsang, Apu Kapadia, Cory Cornelius, and Sean W. Smith. Nymble: Blocking misbehaving users in anonymizing networks. IEEE Transactions on Dependable and Secure Computing, 99(1),2011.
[4]. Lysyanskaya, R.L. Rivest, A. Sahai, and S. Wolf, "Pseudonym Systems," Proc. Conf. Selected Areas in Cryptography, Springer, pp. 184-199, 1999.
[5]. D. Chaum, "Showing Credentials without Identification Transfeering Signatures between Unconditionally Unlinkable Pseudonyms," Proc. Int'l Conf. Cryptology (AUSCRYPT), Springer, pp. 246-264, 1990.
[6]. Nishanth Chandran, Jens Groth, and Amit Sahai. Ring signatures of sub-linear size without random oracles. In ICALP, pages 423–434, 2007.