IJCSC 0973-7391
International Journal of Computer Science & Communication
Volume 6, Issue 2, April-September 2015
ISSN: 0973-7391 Impact Factor: 2.5 Available at www.csjournals.com

Blocking of Mischievous users in Anonymizing Networks using Nymble System

Anil Kumar, Kirti Bhatia
Deptt. of Computer Science & Applications, Sat Kabir Institute of Technology and Management, Ladrawan, Haryana, India
akumar7476@gmail.com, bhatia.kirti.it@gmail.com

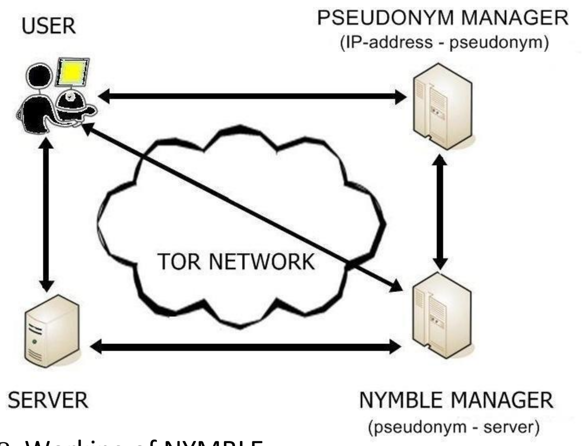
ABSTRACT There are some networks called “Anonymizing Networks” which allow users to gain access to internet services without revealing their identity (IP-addresses) to the servers. Networks such as “Tor (The Onion Router)”,”Crowds” and “I2P” gained popularity in the years 2002-2007, but the success of such networks however has been limited by users employing this anonymity for abusive purposessuch as defacing popular websitessuch as “Wikipedia”. Website Administrators blocks entire network which is connected to the abusive system to get rid of the abuser. Hence, well-behaved users also get blocked due to this action. To address this problem, we present a Nymble system in which servers can “blacklist” mischievous users without affecting good users and also maintaining anonymity across the network.

Keywords: Anonymous, privacy, revocation, pseudonym

1. INTRODUCTION

Networks which provide anonymity to users such as Crowds and Tor [1], [2], will route the traffic through independent nodes in separate administrative domains to hide the user’s IP address. Tor network routes through several series of routers to decrease the probability of predicting the IP address of the user by the server and hence increases the anonymity. But unfortunately some users have misused such networks by taking the advantage of their anonymity to deface popular websites. Since website administrators cannot blacklist individual malicious users’ IP addresses, they blacklist the entire anonymizing network. Such measures will definitely eliminate malicious activity through anonymizing networks, but at the same time it results in denial of service to behaving users as well. In other words, a poisonous fish can kill all other fishes under that same area. (This has happened repeatedly with Tor).

Below is the Nymble system architecture which has various modes of interaction in the network of anonymity. This system has overcome many drawbacks which arise from the previously proposed systems including the speed, computation work, security etc.



2. Working of NYMBLE

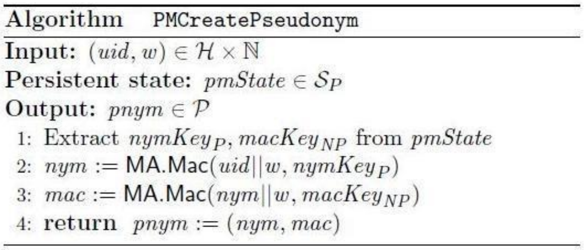
Nymbles are generated by the “Nymble manager” based upon pseudonym and server ID. Websites can blacklist users by obtaining a seed for a particular nymble, allowing them to link future nymbles from the same user. One important thing which can be observed in our proposed system is that even though the future nymbles of the abusive user are linked, the nymbles that are used before complaint remain unlinkable. Hence, Nymble system guarantees backward unlinkability. There are basically three modules in Nymble system. They are:

- Pseudonym Manager
- Nymble Manager
- Blacklisting a user

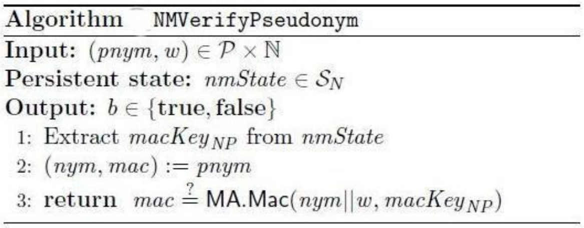
3.The Relationship between Pseudonym Manager, Nymble Manager and Blacklisting a user: User need to contact the **pseudonym manager** and demonstrate control over a particular resource in order to getits IP-address blocked. The user is required to connect to the PM directly i.e. not through a known anonymizing network.

Pseudonym Manager has the knowledge about Tor routers and hence it won’t accept it if a user tries to connect with it with anonymizing network. The basic idea behind connecting directly with Pseudonym Manager is that, it can identify the IP-address of the user. Pseudonyms are chosen based upon the controlled resource ensuring that the same pseudonym is always issued for the same resource. Pseudonym Manager only knows the IP address-pseudonym pair and hence it does not know the server to which the user wants to connect. User contacts the Pseudonym manager only once per link ability window (e.g. Once a day). The Pseudonym Manager issues pseudonyms to users. A pseudonym “pnym” has two components “nym” and “mac”. nym” is a pseudo-random mapping of the user’s

identity, the linkability window w for which the pseudonym is valid and PM's secret key nymKeyp. "mac" is a MAC that the Nymble Manager uses to verify the integrity of the pseudonym.
The below are the algorithms used in creation and verification of pseudonyms.



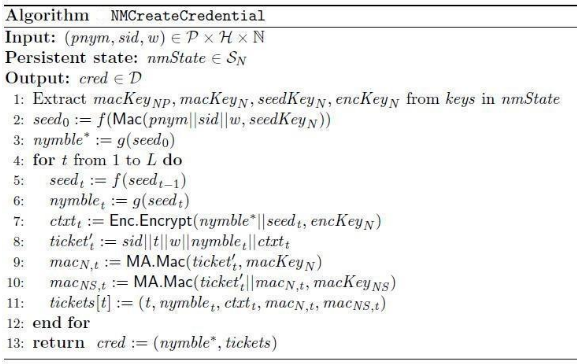
```
Algorithm   PMCreatePseudonym
Input: $(uid, w) \in \mathcal{H} \times \mathbb{N}$
Persistent state: $pmState \in \mathcal{S}_P$
Output: $pnym \in \mathcal{P}$
Extract $nymKey_P, macKey_{NP}$ from $pmState$
$nym := \mathsf{MA.Mac}(uid||w, nymKey_P)$
$mac := \mathsf{MA.Mac}(nym||w, macKey_{NP})$
return  $pnym := (nym, mac)$
```



```
Algorithm   NMVerifyPseudonym
Input: $(pnym, w) \in \mathcal{P} \times \mathbb{N}$
Persistent state: $nmState \in \mathcal{S}_N$
Output: $b \in \{\mathbf{true}, \mathbf{false}\}$
Extract $macKey_{NP}$ from $nmState$
$(nym, mac) := pnym$
return  $mac \overset{?}{=} \mathsf{MA.Mac}(nym||w, macKey_{NP})$
```

After getting the pseudonym from the pseudonym manager, the user connects to the **Nymble manager** through.anonymizing network and requests nymbles for access to a particular server. Nymbles are generated using the user's pseudonym and the server's identity. Nymble Manager doesn't know anything about the user's identity. It knows only the pseudonym-server pair. Nymble Manager encapsulates nymbles within "Nymble tickets" in order to provide cryptographic protection and security properties.

Nymble Tickets are generated based upon the below algorithm.



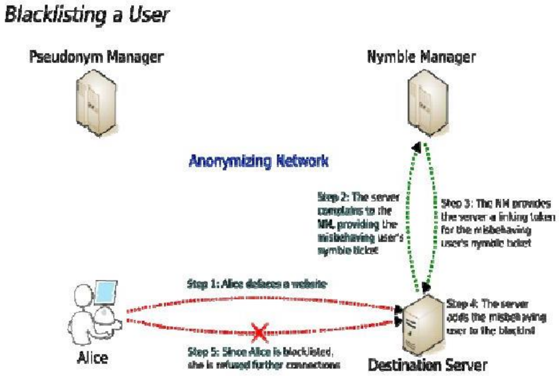
```
Algorithm   NMCreateCredential
Input: $(pnym, sid, w) \in \mathcal{P} \times \mathcal{H} \times \mathbb{N}$
Persistent state: $nmState \in \mathcal{S}_N$
Output: $cred \in \mathcal{D}$
Extract $macKey_{NP}, macKey_N, seedKey_N, encKey_N$ from $keys$ in $nmState$
$seed_0 := f(\mathsf{Mac}(pnym||sid||w, seedKey_N))$
$nymble^* := g(seed_0)$
for $t$ from 1 to $L$ do
    $seed_t := f(seed_{t-1})$
    $nymble_t := g(seed_t)$
    $ctxt_t := \mathsf{Enc.Encrypt}(nymble^*||seed_t, encKey_N)$
    $ticket'_t := sid||t||w||nymble_t||ctxt_t$
    $mac_{N,t} := \mathsf{MA.Mac}(ticket'_t, macKey_N)$
    $mac_{NS,t} := \mathsf{MA.Mac}(ticket'_t||mac_{N,t}, macKey_{NS})$
    $tickets[t] := (t, nymble_t, ctxt_t, mac_{N,t}, mac_{NS,t})$
end for
return  $cred := (nymble^*, tickets)$
```

Whenever a user misbehaves, the server can link any future connection from that user within the current linkability window (e.g. the same day).

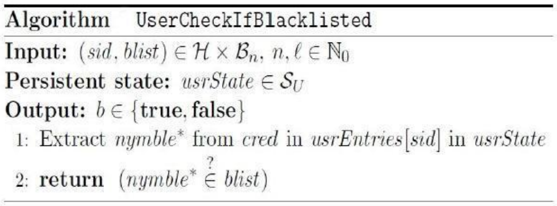
Blacklistability assures that any honest server can indeed block mischievous users.

Specifically, if a honest server complaints about a user that misbehaved in the current linkability window, the complaint will be successful and the user will be not able to nymble-connect to the server successfully in subsequent time periods.

Overview system design:


Blacklisting a User
Pseudonym Manager
Nymble Manager
Anonymizing Network
Step 2: The server complains to the NM, providing the misbehaving user's nymble ticket
Step 3: The NM provides the server a linking token for the misbehaving user's nymble ticket
Step 1: Alice defaces a website
Step 4: The server adds the misbehaving user to the blacklist
Alice
Step 5: Since Alice is blacklisted, she is refused further connections
Destination Server

In the above example, Alice tries to deface a website by using anonymizing network and gets blacklisted by the server. Blacklisting can be implemented by using the below algorithm:

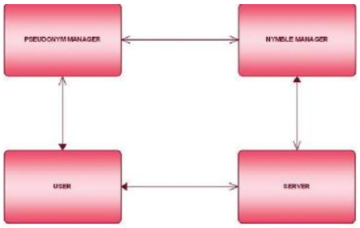


```
Algorithm   UserCheckIfBlacklisted
Input: $(sid, blist) \in \mathcal{H} \times \mathcal{B}_n,\ n, \ell \in \mathbb{N}_0$
Persistent state: $usrState \in \mathcal{S}_U$
Output: $b \in \{\mathbf{true}, \mathbf{false}\}$
Extract $nymble^*$ from $cred$ in $usrEntries[sid]$ in $usrState$
return  $(nymble^* \overset{?}{\in} blist)$
```

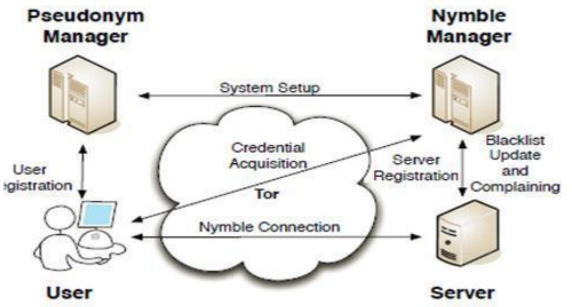
4. PROPOSED WORK

Previously developed systems have so many drawbacks which restricted Tor and other anonymizing networks' usage in the organizations.

Hence, Nymble systems are proposed in order to overcome all those weaknesses and make the Tor a safe and efficient network. In Nymble, users need to acquire an ordered collection of nymbles which is a special type of pseudonym in order to connect with websites. There is no restriction on the type of anonymizing network used i.e. it is not necessary that only Tor should be used here.



Blocking of Mischievous users in Anonymizing Networks using Nymble System



5 CONCLUSIONS

Efficient credential system called Nymble eliminated nearly all weaknesses and drawbacks in the previously developed systems to again make alive anonymizing networks which was blocked by many service providers. Servers can blacklist mischievous users while maintaining their privacy throughout the network. Even though there are still some issues related to backward unlinkability, this system provides enormous security properties. Hope this new system will bring movement in the anonymizing networks' usage andincrease the mainstream acceptance of anonymizing networks such as Tor, Crowds,I2P,etc.which has been completely blocked by several services because of users who abuse their anonymity.

6. 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. Tor Project, available at www.torproject.org, accessed during June 2012.

3. Patrick P. Tsang, Apu Kapadia, and Sean W. Smith, "Nymble: Blocking Misbehaving Users in Anonymizing Networks" IEEE March-April 2011.

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

5. J. Camenisch and A. Lysyanskaya, "An Efficient System for Non-Transferable Anonymous redentials with Optional Anonymity Revocation," Proc. Int'l Conf. Theory and Application of Cryptographic Techniques (EUROCRYPT), Springer, pp. 93-118, 2001.

6. 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.

7. 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.

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

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

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

11. 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.

12. I2P2, available at , www.i2p2.de, accessed during June 2012.