RESEARCH PAPER

Engineering

Volume : 3 | Issue : 8 | Aug 2013 | ISSN - 2249-555X

NYMBLE – A Safe System for Onion Router Networks

KEYWORDS

Nymble, Pseudonym manager, Anonymous Network, Blacklist

S. Murali	Anbarasa Pandian Durai	M. Ariya
Lecturer, Velammal College of Engineering and Technology, Madurai	Assistant Professor, Velammal College of Engineering and Technology, Madurai	Assistant Professor, Velammal College of Engineering and Technology, Madurai

ABSTRACT *An anonymous network such as TOR (The Onion Router) conceals the identities of the users' and by separating identification and routing it conceals the network activity from surveillance and traffic analysis. The network is an implementation of onion routing that encrypts and randomly bounces the communications through a network of relays. Relays are run by the volunteers around the globe. The onion routers employ the encryption in a multi-layered manner so called the onion metaphor and ensure the perfect forward secrecy between relays by providing the users with anonymity in network location. That anonymity uses the Tor's anonymous hidden service feature to extend the hosting of censorship-resistant content.[9] The users can evade the Internet censorship that relies upon blocking public Tor relays[20] by keeping some of the entry relays (bridge relays) secret.*

I. INTRODUCTION

The Onion routing is a technology which is used to provide the anonymous communication between the network entities. The aim of the routing is to provide the low latency connections transparent to the end user by a set of encrypted layers and frequently changing paths between a subset of the routers that participates in the routing system, when the information exchange is resistant against the traffic analysis and other attacks. Users can able to evade Internet censorship relying upon blocking public Tor relays by keeping some of the entry relays secret because the internet address of the sender and the recipient are not in clear text and anyone eavesdropping at any point along the communication channel cannot directly identify the both ends. The exit node is the source node of the communication rather than the sender node.

II. EXISTING SYSTEMS

Anonymous credential systems, employ group signatures. A group signature scheme is used to sign messages anonymously by a group member on behalf of the group. The concept of fingerprinting scheme identifies the buyer of an illegally distributed digital good by providing each buyer with a slightly different version. An anonymous fingerprinting scheme allows the buyer to purchase goods without revealing the identity to the merchant. We propose an efficient anonymous fingerprinting scheme that uses group signature schemes.Backward unlink abilityallows for what we call subjective blacklisting, where servers can blacklist users for whatever reason since the privacy of the blacklisted user is not at risk. In contrast, approaches without backward unlink ability need to pay careful attention to when and why a user must have all their connections linked, and users must worry about whether their behaviors will be judged fairly. In some systems, misbehavior can indeed be defined precisely. Verifier-local revocation (VLR) fixes this shortcoming by requiring the server("verifier") to perform only local updates during revocation.

III. NYMBLE – SAFER SYSTEM

Nymble has the features like rate-limited anonymous connections, revocation auditability (where users can verify whether they have been blacklisted), anonymous authentication, backward unlinkability, subjective blacklisting and fast authentication speeds. In this Nymble system, users acquire a set of nymbles to connect to the Web Servers. These nymbles are logically hard to link, and the collection of nymbles simulates unidentified access to services. Web sites 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 — 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. Our 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.

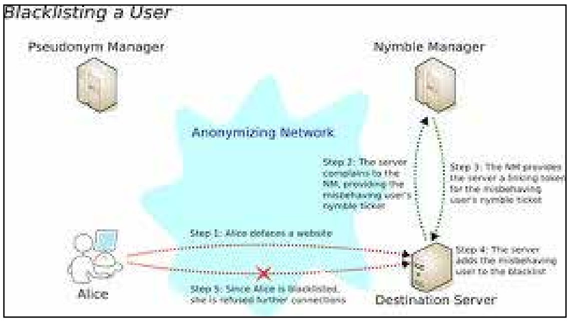
Blacklisting a User
Pseudonym Manager
Nymble Manager
Anonymizing Network
Step 2: The server complains to the NM, providing the misbehaving user's nymble ticket
Step 3: The NM provides the server a linking token for the misbehaving user's nymble ticket
Step 1: Alice defaces a website
Step 4: The server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

Fig. 1.Blacklisting a User

IV. THE PSEUDONYM MANAGER

For IP-address blocking the user must contact the Pseudonym Manager(PM) and requested for the control of resource. Irrespective of any known anonymizing network, the user must connect with the pseudonym manager directly. Based on the controlled resources the pseudonyms are chosen by ensuring that the same pseudonym will be issued for the same type of resource. The server in which the users are connected should not known by them and hence the connection's of the user are anonymous to the pseudonym manager and thereby the mapping of the ip-addresses to the pseudonyms are limited. The user can able to contact with the pseudonym manager through the link ability window.

V. THE NYMBLE MANAGER

The user i.e. Alice can able to connect with the Nymble Manager (NM) through the onion router by the pseudonym and the target server. Hence the ip-address of the user will be hide to the nymble manager but the Pseudonym Manager ensures that some unique ip-address is mapping with the respective pseudonym. Then Alice receives the set of nymble tickets for the server. These nymble tickets are not linkable to each other and hence anonymous access at the target server can be done. Cryptographic protection can be achieved by the nymble ticket. After obtaining a pseudonym from the PM, the user connects to the Nymble Manager (NM) through the

If the server complains in time period tcabout a user's connection in t_, the user becomes linkable starting in tc. The complaint in tccan includes nymble tickets from onlytc_1 and earlier anonymizing network, and requests nymbles for access to particular server (such as Wikipedia).

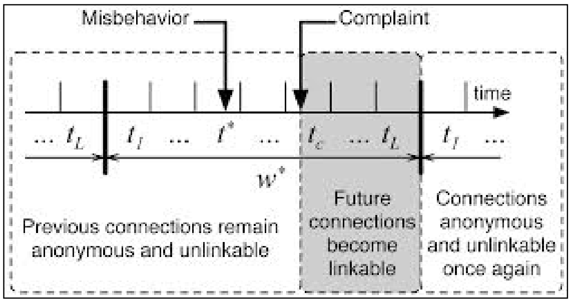
Misbehavior
Complaint
time
... t_L
t_1
...
t^*
...
t_c
... t_L
t_1
...
w^*
Previous connections remain anonymous and unlinkable
Future connections become linkable
Connections anonymous and unlinkable once again

Fig. 2. Linkable and Unlinkable Connections

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 theNM 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 nymbleswithinnymble tickets.

VI. BLACKLISTING A USER

If a user misbehaves, the server may link any future connection from this user within the current linkabilitywindow (e.g., the same day)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 nymbleticket 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 tc; tcþ 1; . . . ; tLofthe 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 (thelinkability window).

The server complaints about the misbehave of the user to the Nymble Manager. Before blacklisting the particular misbehaving user, the Nymble Manager gets the entire details about the user from the Pseudonym Manager which collects the information by means of Pseudo tracker. The Pseudo tracker maintains the identity information and the rating such that if the particular user misbehaved in past, then automatically the rating of the particular user moves down. The Nymble Manager gets the rating of the particular user from the pseudo tracker and if the rating is very high then the user misbehaved for few times only and if the rating is low then the user will be blacklisted.

VII. UPDATION AND VERIFICATION OF BLACKLIST

The server maintains the updated list of the blacklist user for the current time period for two purposes. First one is the server needs to provide the blacklist certificate during the establishment of the new Nymble connection. Second is the server can able to blacklist the particular user based on the recent updation of the list. The updation of the blacklist user is based on the complaints and when there is no complaint the list remains unchanged and it is enough to refresh the server only once. When there is a complaint about the particular user the corresponding entry should be made in the list and the certificates must be regenerated. The updation of the list will be performed at regular time intervals and so multiple updation in the same time is not allowed.

Algorithm .Verification of Blacklist User

```
Input: (sid,t,w,blist,cert) € H x $N^2$ x $β_n$ x C, n €N
Output: b € {true, false}
1: ($t_d$, daisy, $t_s$, mac, sig) :=cert
2: if $t_d$ ≠ t V $t_d$<ts then
3: return false
4: target := $h^{(t_d-t_s)}$ (daisy)
5: content := sid\\$t_s$\\w\\target\\blist
6: return Sig.Verify(content, sig, $verKey_N$)
```

NMComputeBLUpdate algorithm creates new entries to be appended to the server's blacklist. Each entry is either the actual nimble of the user being complained about if the user has not been blacklisted already, or a random nymble otherwise. This way, the server cannot learn if two complaints are about the same user, and thus, cannot link the Nymble connections to the same user.

The BLUpdate algorithm first checks the integrity and freshness of the blacklist and that the NM hasn't already updated the server's blacklist for the current time period. It then checks if all complaints are valid for some previous time period during the current linkability window. Finally, the algorithm prepares an answer to the update request by invoking NMComputeBLUpdate and NMComputeSeeds.

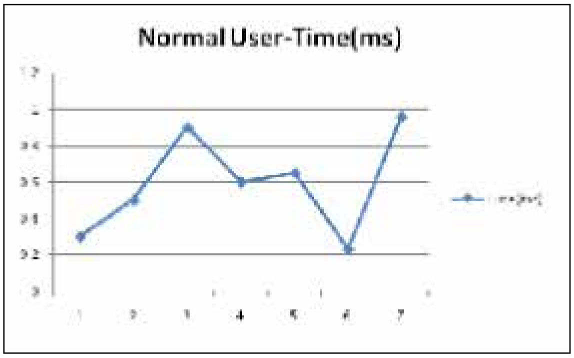

Fig. 2. Variation of Misbehaving User

NMComputeBLUpdate creates new entries to be appended to the server's blacklist. Each entry is either the actual nymble_ of the user being complained about if the user has not been blacklisted already, or a randomnymbleotherwise. This way, the server cannot learn if two complaints are about the same user, and thus, cannot link theNymble connections to the same user. NMComputeSeedsuses the same trick when computing a seed that enables the server to link a blacklisted user.

IX. CONCLUSION

In this paper a new comprehensive credential system called Nymble is proposed and it provides a layer of accountability to any anonymizing network. In this system the server can have the ability to blacklist the misbehaving user with maintaining privacy and in more efficient manner. Our work in this paper will increase the acceptance of anonymizing networks such as the onion router which is blocked by services of anonymous users.

REFERENCE

[1] D. Chaum and E. van Heyst, “Group Signatures,” Proc. Int’l Conf.Theory and Application of Cryptographic Techniques (EUROCRYPT),pp. 257-265, 1991. | | [2] C. Cornelius, A. Kapadia, P.P. Tsang, and S.W. Smith, “Nymble:Blocking Misbehaving Users in AnonymizingNetworks,” Technical Report TR2008-637, Dartmouth College, Computer Science,Dec. 2008. | | [3] I. Damga°rd, “Payment Systems and Credential Mechanisms with Provable Security Against Abuse by Individuals,” Proc. Ann. Int’lCryptology Conf. (CRYPTO), Springer, pp. 328-335, 1988. | | [4] J.R. Douceur, “The Sybil Attack,” Proc. Int’l Workshop on Peer-to-Peer Systems (IPTPS), Springer, pp. 251-260, 2002. | | [5] Jordi Domingo-Pascual; Yuval Shavitt; Steve Uhlig (14 June 2011). Traffic Monitoring and Analysis: Third International Workshop, TMA 2011, Vienna, Austria, April 27, 2011, Proceedings. Springer.pp. 113–.ISBN 978-3-642-20304-6.Retrieved 6 August 2012. | [6] Glater, Jonathan D. (25 January 2006). "Privacy for People Who Don't Show Their Navels".The New York Times.Retrieved 13 May 2011. | |